IBM TotalStorage SAN32M-2

Installation and Service Manual

Service information: 2026 / 432, 32E

Read Before Using

This product contains software that is licensed under written license agreements. Your use of such software is subject to the license agreements under which they are provided.

GC26-7763-03

IBM TotalStorage SAN32M-2

Installation and Service Manual

Service information: 2026 / 432, 32E

GC26-7763-03

Fourth Edition (October 2006)

© Copyright International Business Machines Corporation 2005, 2006. All rights reserved.
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

About this book xiii

Chapter 1 General information

Switch description 1
- Field replaceable units 2
- SFP transceiver 3
- Power supply assembly 4

Controls, connectors, and indicators 5
- RESET button 5
- Ethernet LAN connector 5
- Power and system error LEDs 6
- CRU status LEDs 6
- Maintenance port 6
- Chassis ground connector 6

Switch specifications 7
Maintenance approach 8
Switch management 9
- Management server 9
- Management server specifications 10
- Ethernet hub (optional) 11

Error-detection, reporting, and serviceability features 12
Tools and test equipment 13
- Tools used with the product 13
- Tools supplied by service personnel 15

Chapter 2 Installation tasks

Factory defaults 17
Installation task summary 17
Task 1: Verify installation requirements 19
Task 2: Unpack, inspect, and install the Ethernet hub (optional) 20
- Unpack and inspect Ethernet hub 20
- Desktop installation 21
- Rack-mount installation 22

Task 3: Unpack, inspect, and install the product 24
- Unpack and inspect switch 24
- Desktop installation 24
- Rack-mount installation 25

© Copyright IBM Corp. 2006

Task 4: Configure product using EFCM Basic (optional) 27
Configure product identification 29
Configure date and time 30
Configure parameters 31
Configure fabric parameters 32
Configure network information 34
Configure basic port information 35
Configure port BB_Credit 36
Configure port NPIV 37
Configure SNMP 37
Enable CLI 39
Enable or disable host control 39
Configure SSL encryption 40
Install PFE keys (optional) 42
Configure security 45
Configure interswitch links 46
Task 5: Configure product network information (optional) 47
Task 6: Configure server password and network addresses 50
Configure password 51
Configure private LAN addresses 51
Configure public LAN addresses (optional) 52
Task 7: Configure management server information 53
Access the management server desktop 53
Configure management server names 54
Configure gateway and DNS server addresses 55
Task 8: Configure Windows operating system users 56
Change default administrator password 57
Add a new user 57
Change user properties 58
Task 9: Set management server date and time 59
Task 10: Configure the call-home feature (optional) 61
Task 11: Assign user names and passwords 62
Task 12: Configure the product to the management application 64
Task 13: Record or verify server restore information 65
Task 14: Verify product-to-server communication 66
Task 15: Configure PFE key (optional) 68
Task 16: Configure management server (optional) 70
OSMS 70
FMS 71
Task 17: Set product date and time 72
Task 18: Configure the Element Manager application 74
Configure product identification 75
Configure product parameters 76

Configure fabric parameters....78
Configure ports....80
Configure SNMP....82
Configure threshold alerts....84
Enable EFCM Basic Edition and Telnet access....86
Configure, enable, and test e-mail notification....87
Configure and enable Ethernet events....88
Configure, enable, and test call-home event notification....89
Configure security....89
Configure interswitch links....91
Task 19: Back up configuration data....91
Task 20: Cable Fibre Channel ports....94
Task 21: Configure zoning (optional)....95
Task 22: Connect product to a fabric element (eptional)....96

Chapter 3 Maintenance analysis procedures

Factory defaults....99
Quick start....99
MAP 0000: Start MAP....104
MAP 0100: Power distribution analysis....109
MAP 0200: POST failure analysis....111
MAP 0300: Loss of server communication....113
MAP 0400: Part failure analysis....123
MAP 0500: Port failure or link incident analysis....126
MAP 0600: Fabric or ISL problem analysis....138

Chapter 4 Repair information

Procedural notes....153
Power on switch....153
Power off switch....155
IML or reset switch....155
IML....156
Reset....156
Clean fiber-optic components....157
Download firmware....158
Port LED diagnostics....159
Repair procedures - EFCM Basic Edition....160
Obtain log information....160
Perform port Diagnostics....165
Collect maintenance data....172
Set online state....174

Block or unblock a port 175
Upgrade firmware 176
Manage configuration data 178
Repair procedures - SAN management application 181
Obtain Fabric Log information 181
Obtain Switch Log information 184
Perform port diagnostics 190
Collect maintenance data 200
Set online state 201
Block or unblock a port 202
Upgrade firmware 203
Manage configuration data 206
Install or upgrade software 210

Chapter 5 Removal and replacement procedures

Procedural notes 215
ESD procedures 215
Customer-replaceable unit: SFP optical transceiver 216
Field-replaceable unit: Redundant power supply 220

Chapter 6 Illustrated parts breakdown

Front-accessible FRUs 226
Rear-accessible FRUs 227
Power cords and receptacles 229

Appendix A Event code tables

System events (000 through 199) 234
Power supply events (200 through 299) 254
Fan events (300 through 399) 258
CTP card events (400 through 499) 266
Port events (500 through 599) 272
SBAR Events (600 through 699) 281
Thermal sensor events (800 through 899) 283

Notices 289

Trademarks 291
Electronic emission notices 291
Federal Communications Commission (FCC) Class A Statement 291
Industry Canada Class A Emission Compliance Statement ....

292
Avis de conformité à la réglementation d'Industrie Canada ... 292
European Union (EU) Electromagnetic Compatibility Directive 292
Germany Electromagnetic Compatibility Directive 293
People's Republic of China Class A Electronic Emission Statement 293
Korean Class A Electronic Emission Statement 294
Japan VCCI Class A ITE Electronic Emission Statement 294

Index.....295

Figures

1 SAN32M-2 (front view) 3
2 SAN32M-2 (rear view) 3
3 24-Port Ethernet hub 11
4 Door key 14
5 Loopback plug 14
6 Fiber-optic protective plug 14
7 Null modem cable 15
8 Patch cable and MDI selector configuration 22
9 Mounting bracket installation (Ethernet hub) 23
10 Hardware View 28
11 Identification View 29
12 Date Time View 30
13 Parameters View 31
14 Fabric Parameters View 32
15 Network View 34
16 Basic Information View 36
17 SNMP View 38
18 CLI View 39
19 OSMS View 40
20 SSL View 41
21 Maintenance Feature Installation View 44
22 Connection Description dialog box 48
23 Identification Changes Dialog Box 54
24 Internet Protocol (TCP/IP) Properties dialog box 56
25 Add New User wizard 58
26 Properties dialog box (General tab) 59
27 Date/Time Properties dialog box (Time Zone tab) 60
28 Date/Time Properties dialog box (Date & Time tab) 61
29 Add User dialog box 63
30 Address Properties dialog box (IP Address page) 64
31 Hardware View 67
32 New Feature Key dialog box 69
33 Configure FICON Management Server dialog box 71
34 Configure FICON Management Server Zoning dialog box 72
35 Configure Date and Time dialog box 73
36 Configure Identification dialog box 76
37 Configure Switch Parameters dialog box 77
38 Configure Fabric Parameters dialog box 79
39 Configure Ports dialog box 81

© Copyright IBM Corp. 2006

40 Configure SNMP dialog box 83
41 New Threshold Alert dialog box 85
42 Email Event Notification Setup dialog box 87
43 InCD icon (unformatted CD) 92
44 Daisy-Chained Ethernet Hubs 117
45 Clean fiber-optic components 157
46 Port List View 166
47 Diagnostics View 170
48 System Files View 173
49 Switch View 174
50 Basic Information View 175
51 Firmware Upgrade View 177
52 Backup Configuration View 178
53 Restore Configuration View 179
54 Port List View 191
55 Port Properties dialog box 194
56 Port Technology dialog box 195
57 Port Diagnostics dialog box 196
58 Swap Ports dialog box 199
59 Save Data Collection dialog box 200
60 Set Online State dialog box 202
61 Firmware Library dialog box 204
62 Backup and Restore Configuration dialog box 207
63 Reset Configuration dialog box 208
64 Discover Setup dialog box 209
65 Address Properties dialog box 209
66 InstallShield Wizard dialog box 212
67 SFP optical transceiver removal and replacement 218
68 Redundant power supply removal and replacement 221
69 Front-accessible SFPs 226
70 Rear-accessible FRUs 227
71 Power cords and receptacles 229

Tables

1 IBM products and SAN management documentation—E/OS xiv
2 Factory-set defaults (product) 17
3 Installation task summary 18
4 Operational states and symbols 66
5 Factory-set defaults 99
6 MAP summary 99
7 Event codes versus maintenance action 100
8 MAP 100 event codes 109
9 MAP 200 Event Codes 111
10 MAP 200 Byte 0 CRU Codes 112
11 MAP 300 error messages 116
12 MAP 400 event codes 124
13 MAP 500 event codes 126
14 Link incident messages 127
15 Invalid attachment reasons and actions 128
16 Inactive port reasons and actions 134
17 MAP 600 event codes 139
18 E_Port segmentation reasons and actions 141
19 Port fence codes and actions 146
20 Fabric merge failure reasons and actions 150
21 Port operational states 159
22 Port List Table 166
23 Inspect Port Properties Table 167
24 POM Data Table 168
25 Inspect Port Transceiver Technology Table 168
26 Performance View Table 169
27 Statistical Information in Performance View 192
28 Port Properties Table 193
29 Port Technology Table 195
30 Rear-accessible FRU parts list 228
31 Power cord and receptacle list 230

© Copyright IBM Corp. 2006

About this book

This publication is part of a documentation suite that supports the IBM TotalStorage SAN32M-2 switch.

Who should use this manual

Use this publication if you are a trained installation and service representative experienced with the switch, storage area network (SAN) technology, and Fibre Channel technology.

The IBM TotalStorage SAN32M-2 switch contains no customer-serviceable parts that require internal access to the product during normal operation or prescribed maintenance conditions. In addition, refer to this manual for instructions prior to performing any maintenance action.

Related publications

Other publications that provide additional information about the switch include:

- *IBM TotalStorage Products in a SAN Environment Planning Manual*, GC26-7675.
- *EFC Manager Software Release 8.7 User Manual*, 620-000170.
- *SANavigator Software Release 4.2 User Manual* 621-000013.
- *EFCM Basic Edition User Manual*, 620-000240.
- *SNMP Support Manual*, 620-000131.
- *E/OS Command Line Interface User Manual*, 620-000134.
- *IBM TotalStorage SANC40M Cabinet Installation and Service Manual*, GC26-7746.
- *IBM Systems Safety Notices*, G229-9054.

© Copyright IBM Corp. 2006

IBM and McDATA publications

Some of the documentation that is applicable to IBM TotalStorage products is provided by McDATA Corporation. The documents often are identified by a McDATA product name that corresponds to the IBM product name. Table 1 lists the IBM product name, the corresponding McDATA product name, the applicable software, and the documentation that is relevant to the product.

Table 1 IBM products and SAN management documentation—E/OS

IBM TotalStorage product name, and machine type and model	McDATA product name	Related firmware and SAN management product	Relevant documentation
SAN12M-1 Switch • 2026-E12 • 2026-12E	Sphereon 4300 Switch	• E/OS • EFCM Basic Edition	• *EFCM Basic Edition User Manual* (620-000240) • *E/OS SNMP Support Manual* (620-000131) • *E/OS Command Line Interface User Manual* (620-000134)
SAN24M-1 Switch • 2026-224	Sphereon 4500 Switch	• E/OS • EFCM • Element Manager • EFCM Basic Edition	• *EFC Manager Software Release 8.7 User Manual,* 620-000170. • *Sphereon 4500 Switch Element Manager User Manual* (620-000175) • *EFCM Basic Edition User Manual* (620-000240) • *E/OS SNMP Support Manual* (620-000131) • *E/OS Command Line Interface User Manual* (620-000134)
SAN32M-1 Switch • 2027-232	Sphereon 3232 Switch	• E/OS • EFCM • Element Manager • EFCM Basic Edition	• *EFC Manager Software Release 8.7 User Manual,* 620-000170. • *Sphereon 3032 and 3232 Fabric Switch Element Manager User Manual* (620-000173) • *EFCM Basic Edition User Manual* (620-000240) • *E/OS SNMP Support Manual* (620-000131) • *E/OS Command Line Interface User Manual* (620-000134)
SAN16M-2 Switch • 2026-416 • 2026-16E	Sphereon 4400 Switch	• E/OS • EFCM • Element Manager • EFCM Basic Edition	• *EFC Manager Software Release 8.7 User Manual,* 620-000170. • *Sphereon 4400 Switch Element Manager User Manual* (620-000241) • *EFCM Basic Edition User Manual* (620-000240) • *E/OS SNMP Support Manual* (620-000131) • *E/OS Command Line Interface User Manual* (620-000134)

Table 1 IBM products and SAN management documentation—E/OS (Continued)

IBM TotalStorage product name, and machine type and model	McDATA product name	Related firmware and SAN management product	Relevant documentation
SAN32M-2 Switch • 2026-432 • 2026-32E	Sphereon 4700 Switch	• E/OS • EFCM • Element Manager • EFCM Basic Edition	• *EFC Manager Software Release 8.7 User Manual*, 620-000170. • *Sphereon 4700 Switch Element Manager User Manual* (620-000242) • *EFCM Basic Edition User Manual* (620-000240) • *E/OS SNMP Support Manual* (620-000131) • *E/OS Command Line Interface User Manual* (620-000134)
SAN140M director • 2027-140	Intrepid 6140 director	• E/OS • EFCM • Element Manager • EFCM Basic Edition	• *EFC Manager Software Release 8.7 User Manual*, 620-000170. • *Intrepid 6140 and 6064 Directors Element Manager User Manual* (620-000153) • *EFCM Basic Edition User Manual* (620-000240) • *E/OS SNMP Support Manual* (620-000131) • *E/OS Command Line Interface User Manual* (620-000134)

Ordering manuals

To order a printed copy of this publication, contact your IBM Branch office or you can locate (and purchase) books online at: http://www.elink.ibmlink.ibm.com/public/applications/publications/cgibin/pbi.cgi?

Where to get help

Contact IBM for technical support, which includes hardware support, all product repairs, and ordering of spare parts, go to: http://www.ibm.com/servers/storage/support/san/index.html.

You can also contact IBM within the United States at 1-800-IBMSERV (1-800-426-7378). For support outside the United States, you can find the service number at http://www.ibm.com/planetwide/.

Taiwan contact information

IBM Taiwan Product Service Contact Info:

IBM Taiwan Corporation
3F, No 7, Song Ren Rd., Taipei Taiwan
Tel: 0800-016-888

台灣IBM 產品服務聯絡方式：
台灣國際商業機器股份有限公司
台北市松仁路7號3樓
電話：0800-016-888

How to send your comments

Your feedback is important in helping us provide the most accurate and high-quality information. If you have comments or suggestions for improving this document, you can send us comments electronically by using the following addresses:

- Internet: starpubs@us.ibm.com
- IBMLink™ from U.S.A.: STARPUBS at SJEVM5
- IBMLink from Canada: STARPUBS at TORIBM
- IBM Mail Exchange: USIB3VVD at IBMMAIL

You can also mail your comments by using the Reader Comment Form in the back of this manual or direct your mail to:

International Business Machine Corporation
Information Development
Department GZW
9000 South Rita Road
Tucson, Arizona 85744-001 U.S.A

When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

Safety and environmental notices

ATTENTION ! The SAN32M-2 is designed to be installed by customers. It has no customer-serviceable parts, however, and must be serviced by qualified service representatives.

Safety notices and labels

When using this product, observe the danger, caution, and attention notices contained in this guide. The notices are accompanied by symbols that represent the severity of the safety condition. The danger and caution notices are listed in numerical order based on their IDs, which are displayed in parentheses, for example (D004), at the end of each notice. Use this ID to locate the translations of these danger and caution notices in the *IBM Safety Notices* (G229-9054) publication, which is on the CD-ROM that accompanies this product.

The following notices and statements are used in this document. They are listed below in order of increasing severity of potential hazards. Follow the links for more detailed descriptions and examples of the danger, caution, and attention notices in the sections that follow.

- **Note:** These notices provide important tips, guidance, or advice.
- **Attention notices:** These notices indicate potential damage to programs, devices, or data.
- **Caution notices:** These statements indicate situations that can be potentially hazardous to you.
- **Danger notices:** These statements indicate situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these situations.

Danger notices

A danger notice calls attention to a situation that is potentially lethal or extremely hazardous to people. A lightning bolt symbol accompanies a danger notice to represent a dangerous electrical condition. Read and comply with the following danger notices before installing or servicing this device.

DANGER

To prevent a possible shock from touching two surfaces with different protective ground (earth), use one hand, when possible, to connect or disconnect signal cables.
(D001)

DANGER

Overloading a branch circuit is potentially a fire hazard and a shock hazard under certain conditions. To avoid these hazards, ensure that your system electrical requirements do not exceed branch circuit protection requirements. Refer to the information that is provided with your device or the power rating label for electrical specifications.
(D002)

DANGER

If the receptacle has a metal shell, do not touch the shell until you have completed the voltage and grounding checks. Improper wiring or grounding could place dangerous voltage on the metal shell. If any of the conditions are not as described, STOP. Ensure the improper voltage or impedance conditions are corrected before proceeding.
(D003)

DANGER

An electrical outlet that is not correctly wired could place hazardous voltage on metal parts of the system or the devices that attach to the system. It is the responsibility of the customer to ensure that the outlet is correctly wired and grounded to prevent an electrical shock.
(D004)

A comprehensive danger notice provides instructions on how to avoid shock hazards when servicing equipment. Unless instructed otherwise, follow the procedures in the following danger notice.

DANGER

Electrical voltage and current from power, telephone, and communication cables are hazardous. To avoid a shock hazard:

- ***Do not connect or disconnect any cables or perform installation, maintenance, or reconfiguration of this product during an electrical storm.***
- ***Connect all power cords to a properly wired and grounded electrical outlet. Ensure outlet supplies proper voltage and phase rotation according to the system rating plate.***
- ***Connect any equipment that will be attached to this product to properly wired outlets.***
- ***When possible, use one hand only to connect or disconnect signal cables.***
- ***Never turn on any equipment when there is evidence of fire, water, or structural damage.***
- ***Disconnect the attached power cords, telecommunications systems, networks, and modems before you open the device covers, unless instructed otherwise in the installation and configuration procedures.***
- ***Connect and disconnect cables as described below when installing, moving, or opening covers on this product or attached devices.***

To Disconnect:

1. ***Turn everything OFF (unless instructed otherwise).***
2. ***Remove power cords from the outlet.***
3. ***Remove signal cables from connectors.***
4. ***Remove all cables from devices.***

To Connect:

1. ***Turn everything OFF (unless instructed otherwise).***
2. ***Attach all cables to devices.***
3. ***Attach signal cables to connectors.***
4. ***Attach power cords to outlet.***
5. ***Turn device ON.***

(D005)

Labels

As an added precaution, safety labels are often installed directly on products or product components to warn of potential hazards. These

can be either danger or caution notices, depending upon the level of the hazard.

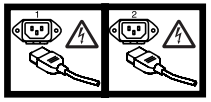
The actual product safety labels may differ from these sample safety labels:

DANGER

Hazardous voltage, current, or energy levels are present inside any component that has this label attached.
(L001)

DANGER

Rack-mounted devices are not to be used as a shelf or work space.
(L002)



DANGER

Multiple power cords
(L003)

Caution notices

A caution notice calls attention to a situation that is potentially hazardous to people because of some existing condition. A caution notice can be accompanied by different symbols, as in the examples below:

If the symbol is...	It means....
	A hazardous electrical condition with less severity than electrical danger.
	A generally hazardous condition not represented by other safety symbols.
>18kg (39.7 lb)	A specification of product weight that requires safe lifting practices. The weight range of the product is listed below the graphic, and the wording of the caution varies, depending on the weight of the device.
Class I	A hazardous condition due to the use of a laser in the product. Laser symbols are always accompanied by the classification of the laser as defined by the U. S. Department of Health and Human Services (for example, Class I, Class II, and so forth).

Read and comply with the following caution notices before installing or servicing this device.

CAUTION

This part or unit is heavy, but has a weight smaller than 18 kg (39.7 lb.). Use care when lifting, removing, or installing this part or unit.
(C008)

CAUTION

The doors and covers to the product are to be closed at all times except for service by trained service personnel. All covers must be replaced and doors locked at the conclusion of the service operation.
(C013)

CAUTION

The system contains circuit cards and/or assemblies that contain lead solder. To avoid the release of lead (Pb) into the environment, do not burn. Discard the circuit card as instructed by local regulations.
(C014)

CAUTION

Ensure the building power circuit breakers are turned off BEFORE you connect the power cord(s) to the building power.
(C023)

CAUTION

This assembly contains mechanical moving parts. Use care when servicing this assembly.
(C025)

CAUTION

Servicing of this product or unit is to be performed by trained service personnel only.
(C032)

Attention notices

An attention notice indicates the possibility of damage to a program, device, or system, or to data. An exclamation point symbol may accompany an attention notice, but is not required. A sample attention notice follows:

ATTENTION ! Do not bend a fibre cable to a radius less than 5 cm (2 in.); you can damage the cable. Tie wraps are not recommended for optical cables because they can be easily overtightened, causing damage to the cable.

Laser safety

This equipment contains Class 1 laser products, and complies with FDA radiation Performance Standards, 21 CFR Subchapter J and the international laser safety standard IEC 60825.

CAUTION

This product may contain one or more of the following: CD-ROM, DVD-ROM, DVD-RAM, or laser module, which are Class 1 laser products. Please note the following:

- **Do not remove the covers. Removing the covers of the laser product could result in exposure to hazardous laser radiation. There are no serviceable parts inside the device.**
- **Use of the controls or adjustments or performance of procedures other than those specified herein might result in hazardous radiation exposure.**

(C026)

CAUTION

Data processing environments can contain equipment transmitting on system links with laser modules that operate at greater than Class 1 power levels. For this reason, never look into the end of an optical fiber cable or open receptacle.

(C027)

Environmental notices

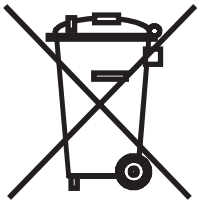
Use the environmental statements and warning in this section to guide you when using this product and in properly disposing of the product and its components.

Product recycling and disposal

This unit must be recycled or discarded according to applicable local and national regulations. IBM encourages owners of information technology (IT) equipment to responsibly recycle their equipment when it is no longer needed. IBM offers a variety of product return programs and services in several countries to assist equipment owners in recycling their IT products. Information on IBM product recycling offerings can be found on IBM's Internet site at http://www.ibm.com/ibm/environment/products/prp.shtml

Esta unidad debe reciclarse o desecharse de acuerdo con lo establecido en la normativa nacional o local aplicable. IBM

recomienda a los propietarios de equipos de tecnología de la información (TI) que reciclen responsablemente sus equipos cuando éstos ya no les sean útiles. IBM dispone de una serie de programas y servicios de devolución de productos en varios países, a fin de ayudar a los propietarios de equipos a reciclar sus productos de TI. Se puede encontrar información sobre las ofertas de reciclado de productos de IBM en el sitio web de IBM http://www.ibm.com/ibm/environment/products/prp.shtml.



Note: This mark applies only to countries within the European Union (EU) and Norway.

Appliances are labeled in accordance with European Directive 2002/96/EC concerning waste electrical and electronic equipment (WEEE). The Directive determines the framework for the return and recycling of used appliances as applicable throughout the European Union. This label is applied to various products to indicate that the product is not to be thrown away, but rather reclaimed upon end of life per this Directive.

注意：このマークは EU 諸国およびノルウェーにおいてのみ適用されます。

この機器には、EU 諸国に対する廃電気電子機器指令 2002/96/EC(WEEE) のラベルが貼られています。この指令は、EU 諸国に適用する使用済み機器の回収とリサイクルの骨子を定めています。このラベルは、使用済みになった時に指令に従って適正な処理をする必要があることを知らせるために種々の製品に貼られています。

Remarque : Cette marque s'applique uniquement aux pays de l'Union Européenne et à la Norvège.

L'étiquette du système respecte la Directive européenne 2002/96/EC en matière de Déchets des Equipements Electriques et Electroniques (DEEE), qui détermine les dispositions de retour et de recyclage applicables aux systèmes utilisés à travers l'Union européenne. Conformément à la directive, ladite étiquette précise que le produit sur lequel elle est apposée ne doit pas être jeté mais être récupéré en fin de vie.

In accordance with the European WEEE Directive, electrical and electronic equipment (EEE) is to be collected separately and to be

reused, recycled, or recovered at end of life. Users of EEE with the WEEE marking per Annex IV of the WEEE Directive, as shown above, must not dispose of end of life EEE as unsorted municipal waste, but use the collection framework available to customers for the return, recycling and recovery of WEEE. Customer participation is important to minimize any potential effects of EEE on the environment and human health due to the potential presence of hazardous substances in EEE. For proper collection and treatment, contact your local IBM representative.

Battery return program

This product may contain sealed lead acid, nickel cadmium, nickel metal hydride, lithium, or lithium ion battery. Consult your user manual or service manual for specific battery information. The battery must be recycled or disposed of properly. Recycling facilities may not be available in your area. For information on disposal of batteries outside the United States, go to http://www.ibm.com/ibm/environment/products/batteryrecycle.shtml or contact your local waste disposal facility.

In the United States, IBM has established a return process for reuse, recycling, or proper disposal of used IBM sealed lead acid, nickel cadmium, nickel metal hydride, and other battery packs from IBM Equipment. For information on proper disposal of these batteries, contact IBM at 1-800-426-4333. Please have the IBM part number listed on the battery available prior to your call.

For Taiwan:

Cable warning

WARNING

Handling the cord on this product or cords associated with accessories sold with this product, will expose you to lead, a chemical known to the State of California to cause cancer, and birth defects or other reproductive harm. Wash hands after handling.

Chapter 1: General information

The IBM TotalStorage SAN32M-2 switch provides 32 ports of low-cost and high-performance dynamic Fibre Channel connectivity for switched fabric or arbitrated loop devices. This function allows low-cost, low-bandwidth workgroup (edge) devices to communicate with mainframe servers, mass storage devices, or other peripherals, and ultimately be incorporated into an enterprise storage area network (SAN) environment.

The IBM TotalStorage SAN32M-2 switch will be referred to throughout the rest of the manual as the SAN32M-2, or simply the *switch*.

This chapter describes:

- The switch, including customer-replaceable units (CRUs), controls, connectors, indicators, and specifications.
- Maintenance approach.
- Switch management.
- Error detection, reporting, and serviceability features.
- Tools and test equipment.

Switch description

The switch provides Fibre Channel connectivity through generic mixed ports (GX_Ports). Ports operate at 1.0625, 2.1250, or 4.2500 gigabits per second (Gbps), and can be configured as:

- Fabric ports (F_Ports) to provide direct connectivity for switched fabric devices.
- Expansion ports (E_Ports) to provide interswitch link (ISL) connectivity to fabric directors and switches.
- Fabric loop ports (FL_Ports) to provide connectivity and fabric attachment for Fibre Channel arbitrated loop (FC-AL) devices.

The switch is installed on a table or desktop, or mounted in a standard 19-inch equipment rack.

© Copyright IBM Corp. 2006

Operators with a browser-capable PC and Internet connectivity can manage the switch through a firmware-resident Enterprise Fabric Connectivity Manager (EFCM) Basic Edition interface. The interface manages only a single switch, and provides a graphical user interface (GUI) that supports configuration, statistics monitoring, operation, and maintenance. The interface is opened from a web browser running Netscape Navigator® 4.6 (or higher) or Microsoft® Internet Explorer 4.0 (or higher).

As an option, the switch is managed through a one-unit (1U) high, rack-mount management server running a Java™-based SAN management application (SANavigator® 4.2 or EFCM 8.7 or later) and the switch Element Manager application.

Multiple switches and the management server communicate on a local area network (LAN) through one or more 10/100 Base-T Ethernet hubs. The 24-port Ethernet hubs are optional and ordered with the switch. Up to three hubs are daisy-chained as required to provide additional Ethernet connections as more switches (or other managed products) are installed on a network.

Field replaceable units

The switch provides a modular design that enables quick removal and replacement of FRUs, including small form factor pluggable (SFP) optical transceivers and power supply assemblies. Figure 1 illustrates the front of the switch and shows the:

1. Ethernet LAN connector.
2. **RESET** button.
3. Chassis ground (**GND**) connector.
4. Green power (**PWR**) light-emitting diode (LED).
5. Amber system error (**ERR**) LED.
6. SFP optical transceivers (32).

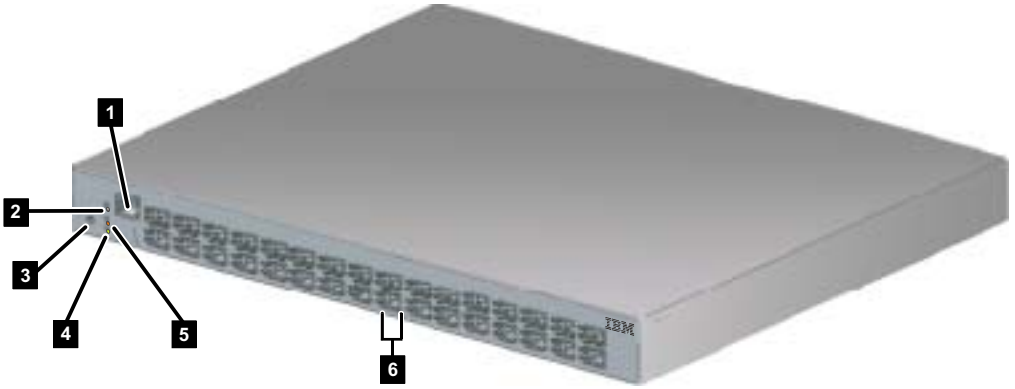


Figure 1 SAN32M-2 (front view)

Figure 2 illustrates the rear of the switch and shows the:

1. RS-232 maintenance port.
2. Power supply assemblies with internal cooling fans (2).

Figure 2 SAN32M-2 (rear view)

SFP transceiver

Singlemode or multimode fiber-optic cables attach to switch ports through SFP transceivers. The fiber-optic transceivers provide duplex LC® connectors, and can be detached from switch ports (through a 10-pin interface) for easy replacement.

Tri-rate shortwave laser transceive types (1.0625, 2.1250, or 4.2500 Gbps) are also available. Shortwave laser transceivers (850 nm) provide connectivity:

- At 500 meters (1.0625 Gbps) through 50-micron multimode fiber-optic cable.
- At 300 meters (2.1250 Gbps) through 50-micron multimode fiber-optic cable.
- At 150 meters (4.2500 Gbps) through 50-micron multimode fiber-optic cable.
- At 300 meters (1.0625 Gbps) through 62.5-micron multimode fiber-optic cable.
- At 150 meters (2.1250 Gbps) through 62.5-micron multimode fiber-optic cable.
- At 70 meters (4.2500 Gbps) through 62.5-micron multimode fiber-optic cable.

Tri-rate longwave laser (1.0625, 2.1250, or 4.2500 Gbps) are also available. Longwave laser transceivers provide connectivity at 4 kilometers and 10 kilometers through singlemode fiber-optic cable.

The switch also provides a predictive optics monitoring (POM) feature that monitors operation of SFP optical transceivers. Digital diagnostics-enabled optical transceivers report temperature, voltage current, transceiver power, and receiver power to product firmware. Optical transceivers also provide vendor-specific threshold values for these parameters.

Power supply assembly

The switch contains two power supply assemblies with internal cooling fans. These redundant, load-sharing assemblies step down and rectify facility input power to provide 12 volts direct current (VDC) to the control processor (CTP) card. The power supplies also provide input filtering, overvoltage protection, and overcurrent protection.

Either power supply can be replaced while the switch is operational. Each power supply has a separate connection to the CTP card to allow for independent AC power sources. The power supplies are input rated at 90 to 264 volts alternating current (VAC).

Three cooling fans integrated in each power supply (six fans total) provide cooling for the power supplies and CTP card, as well as redundancy for continued operation if a single fan fails. Fans are removed and replaced as part of the integrated power supply.

Controls, connectors, and indicators

Controls, connectors, and indicators for the switch include the:

- **RESET** button.
- Ethernet LAN connector.
- Green **PWR** and amber **ERR** LEDs.
- Green and amber status LEDs associated with CRUs.
- RS-232 maintenance port.
- Chassis ground (**GND**) connector.

RESET button

When the **RESET** button is pressed, held for three seconds, and released, the switch performs an initial machine load (IML) that reloads the firmware from FLASH memory. This operation is not disruptive to Fibre Channel traffic. When the **RESET** button is pressed and held for ten seconds, the switch performs a reset. After three seconds, the **ERR** LED blinks at twice the unit beaconing rate. A reset is disruptive to Fibre Channel traffic and resets the:

- Microprocessor and functional logic for the CTP card and reloads the firmware from FLASH memory.
- Ethernet LAN interface, causing the connection to the management server to drop momentarily until the connection automatically recovers.
- Ports, causing all Fibre Channel connections to drop momentarily until the connections automatically recover. This causes attached devices to log out and log back in, therefore data frames lost during switch reset must be retransmitted.

Perform a reset only if a CTP card failure is indicated. The button is flush mounted to protect against inadvertent activation.

Ethernet LAN connector

The front panel has a 10/100 megabit per second (Mbps) RJ-45 twisted-pair connector that attaches to an Ethernet LAN to provide communication with a management server or simple network management protocol (SNMP) workstation.

The connector provides two green LEDs. The left LED illuminates to indicate LAN operation at 10 Mbps. The right LED illuminates to indicate operation at 100 Mbps.

Power and system error LEDs

The **PWR** LED illuminates when the switch is connected to facility AC power and is operational (the product does not have a power switch). If the LED extinguishes, a facility power source, power cord, or power distribution failure is indicated.

The **ERR** LED illuminates when the switch detects an event requiring operator attention, such as a CRU failure. The LED illuminates as long as an event is active. The LED extinguishes when *Clear System Error Light* is selected from the EFCM Basic Edition interface or Element Manager application. The **ERR** LED also blinks if unit beaconing is enabled. An illuminated LED (indicating a failure) takes precedence over unit beaconing.

CRU status LEDs

Amber and green LEDs associated with switch CRUs provide status information as follows:

- **Fibre Channel ports -** LEDs to the left of each port illuminate, extinguish, or blink to indicate port status and speed. The amber LED illuminates if the port fails. The green LED illuminates to indicate 1.0625, 2.1250, or 4.2500 Gbps port operation.
- **Power supply assembly -** An amber LED on each assembly illuminates if the FRU fails.

Maintenance port

The rear panel has a 9-pin DSUB maintenance port that provides a connection for a local terminal or dial-in connection for a remote terminal. The port is typically used only by maintenance personnel, however operators can use the port to configure network addresses.

Chassis ground connector

The front panel has a chassis ground connector for an electrostatic discharge (ESD) wrist strap and grounding cable. Plug the grounding cable into the connector when performing a maintenance action with the switch connected to facility power (grounded).

Switch specifications

This section lists physical characteristics, storage and shipping environment, operating environment, and service clearances.

Physical characteristics

Dimensions:

Height: 4.1 centimeters (1.6 inches) or 1 rack unit

Width: 43.7 centimeters (17.2 inches)

Depth: 39.4 centimeters (15.5 inches)

Weight: 6.8 kilograms (15.0 pounds)

Power requirements:

Input voltage: 90 to 264 VAC

Input current: 0.35 amps at 208 VAC

Input frequency: 47 to 63 Hz

Heat dissipation:

71 watts (242 BTUs/hr)

Cooling airflow clearances (switch chassis):

Right and left side: 1.3 centimeters (0.5 inches)

Front and rear: 7.6 centimeters (3.0 inches)

Top and bottom: No clearance required

Shock and vibration tolerance:

60 Gs for 10 milliseconds without nonrecoverable errors

Acoustical noise:

70 dB "A" scale

Inclination:

10^0 maximum

Storage and shipping environment

Protective packaging must be provided to protect the switch under all shipping methods (domestic and international).

Shipping temperature:

-40^0 C to 60^0 C (-40^0 F to 140^0 F)

Storage temperature:

1^0 C to 60^0 C (34^0 F to 140^0 F)

Shipping relative humidity:

5% to 100%

Storage relative humidity:

5% to 80%

Maximum wet-bulb temperature:

29^0 C (84^0 F)

Altitude:

12,192 meters (40,000 feet)

Operating environment

Temperature:

4^0 C to 40^0 C (40^0 F to 104^0 F)

Relative humidity:

8% to 80%

Maximum wet-bulb temperature:

27^0 C (81^0 F)

Altitude:

3,048 meters (10,000 feet)

Maintenance approach

The maintenance approach instructs service personnel to perform fault isolation and repair procedures without degrading or interrupting product operation or associated applications. Fault isolation begins when one or more of the following occur:

- Event information displays at a browser-capable PC communicating with the product through the EFCM Basic Edition interface.
- Event information displays at a LAN-connected PC or workstation communicating with the rack-mount management server running a SAN management application.

- LEDs on the product front panel or CRUs illuminate to indicate a hardware malfunction.
- An unsolicited SNMP trap message is received at a management workstation, indicating an operational state change or failure.
- Event notification is received at a designated support center through an e-mail message or the call-home feature.

Fault isolation and repair information is provided through maintenance analysis procedures (MAPs). MAPs are step-by-step procedures that provide information to interpret events, isolate a failure to a CRU, remove and replace the CRU, and verify product operation. Fault isolation begins with *MAP 0000: Start MAP*.

Switch management

The switch is managed and controlled through a:

- Customer-supplied PC platform with Internet communication to the product-resident EFCM Basic Edition interface.

  The interface allows service personnel to perform configuration tasks, view system alerts and related log information, and monitor switch status, port status, and performance. CRU status and system alert information are highly visible.

- Optional management server (running a SAN management application) that provides a central point of control for up to 48 switches or managed products.

  A customer-supplied PC or workstation (with client applications installed) communicates with the server through a through a corporate intranet.

- Customer-supplied PC or UNIX-based platform with the server and client SAN management and Element Manager applications installed by the customer.

Management server

An optional management server can be installed to run EFCM Basic. The minimum specifications are described below.

Management server specifications

This section summarizes minimum and recommended hardware specifications for a management server. Servers may ship with more enhanced hardware, such as a faster processor, additional random-access memory (RAM), or a higher-capacity hard drive.

Minimum specifications

Minimum server specifications are:

- A rack-mount server running the Intel® Pentium® 4 processor with a 2 gigahertz (GHz) or greater clock speed, using the Microsoft Windows 2000 Professional (with service pack 4), Windows XP Professional (with service pack 2), or Windows Server 2003 operating system (Enterprise Edition with service pack 1) operating system.
- TightVNC™ Viewer Version 1.2.7 client-server software control package that provides remote network access (through a web browser) to the management server desktop.
- 1,024 megabyte (MB) RAM.
- 40 gigabyte (GB) internal hard drive.
- 1.44 MB 3.5-inch slim-type disk drive.
- 24X read speed slim-type compact disk-rewritable (CD-RW) and 8X read speed digital video disk (DVD) combination drive, data only.
- 56K peripheral component interconnect (PCI) internal data and fax modem, using the V .92 dial-up specification.
- 16 MB graphics card.
- Network interface card (NIC) with two 10/100 Mbps Ethernet adapters using RJ-45 connectors.

Recommended specifications

Recommended server specifications are:

- A rack-mount server running the Intel Pentium 4 processor with a 3 GHz or greater clock speed, using an 800 megahertz (MHz) front side bus, using the Microsoft Windows Server 2003 operating system (Enterprise Edition with service pack 1).
- TightVNC™ Viewer Version 1.2.7 client-server software control package that provides remote network access (through a web browser) to the management server desktop.

- 2,048 MB (or greater) double data-rate synchronous dynamic random access memory (SDRAM).
- 40 GB (or greater) internal hard drive, with advanced technology attachment (ATA-100) integrated drive electronics interface operating at 7,200 rpm.
- 1.44 MB 3.5-inch slim-type disk drive.
- 48X read speed slim-type CD-RW and 32X read speed DVD combination drive, data only.
- 56K PCI internal data and fax modem, using the V .92 dial-up specification.
- Video graphics array (VGA) capable 32 MB graphics card.

NIC with two 10/100 Mbps Ethernet adapters using RJ-45 connectors.

Ethernet hub (optional)

The management server and managed switches connect through a 10/100 Base-T Ethernet hub. Figure 3 illustrates the 24-port hub.

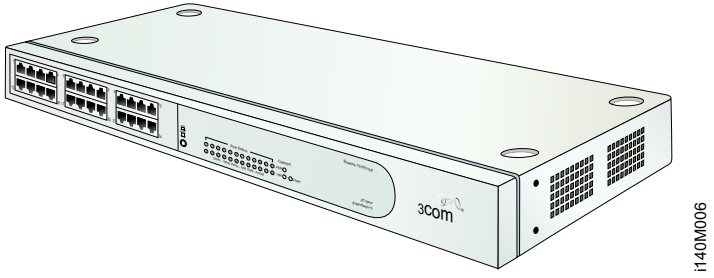


Figure 3 24-Port Ethernet hub

Hubs can be daisy-chained to provide additional connections as more switches (or other IBM-managed products) are installed on a network. Multiple hubs are daisy-chained by attaching RJ-45 Ethernet patch cables and configuring each hub through a medium-dependent interface (MDI) switch.

Error-detection, reporting, and serviceability features

The switch provides the following error detection, reporting, and serviceability features:

- LEDs on switch CRUs and adjacent to Fibre Channel ports that provide visual indicators of hardware status or malfunctions.
- Redundant CRUs and FRUs (SFP transceivers and integrated cooling fan and power supply assemblies) that are removed or replaced without disrupting switch or Fibre Channel link operation.
- A modular design that enables quick removal and replacement of CRUs without the use of tools or equipment.
- System alerts and logs that display switch, Ethernet link, and Fibre Channel link status at the EFCM Basic Edition interface, client communicating with the management server, or customer-supplied server (running a SAN management application).
- Diagnostic software that performs power-on self-tests (POSTs) and port diagnostics (loopback tests).
- An RS-232 maintenance port at the rear of the switch (port access is password protected) that enables installation or service personnel to change the switch's IP address, subnet mask, and gateway address.

  These parameters can also be changed through a Telnet session, access for which is provided through a local or remote PC with an Internet connection to the switch.
- Data collection through the EFCM Basic Edition interface or Element Manager application to help isolate system problems. The data includes a memory dump file and audit, hardware, and engineering logs.
- Beaconing to assist service personnel in locating a specific port or switch. When port beaconing is enabled, the amber LED associated with the port flashes. When unit beaconing is enabled, the system error indicator on the front panel flashes. Beaconing does not affect port or switch operation.
- An internal modem for use by support personnel to dial-in to the management server (optional) for event notification and to perform remote diagnostics.

- Automatic notification of significant system events (to support personnel or administrators) through e-mail messages or the call-home feature.

  NOTE: Call home may not be available with the enterprise version of EFCM if the customer server does not have a modem.

- SNMP management using the Fibre Channel Fabric Element MIB, Transmission Control Protocol/Internet Protocol (TCP/IP) MIB-II definition (RFC 1157), or a product-specific private enterprise MIB that runs on the switch. Up to six authorized management workstations can be configured through the EFCM Basic Edition interface or Element Manager application to receive unsolicited SNMP trap messages. The trap messages indicate product operational state changes and failure conditions.
- Optional SNMP management using the Fibre Alliance MIB that runs on the management server. Up to 12 authorized management workstations can be configured through the SAN management application to receive unsolicited SNMP trap messages. The trap messages indicate operational state changes and failure conditions.

Tools and test equipment

This section describes tools and test equipment that may be required to install, test, service, and verify operation of the product and attached management server. These tools are supplied with the product or must be supplied by service personnel.

Tools used with the product

The following tools may be used to service the product:

- **Door key -** A door key with 5/16-inch socket (Figure 4) may be required to open front and rear doors of the equipment cabinet. A 5/16-inch socket wrench may also be used.

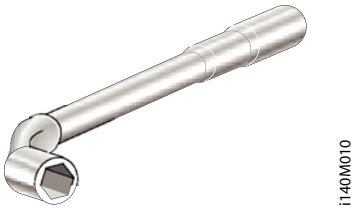


Figure 4 **Door key**

- **Loopback plug -** A multimode (shortwave laser) or singlemode (longwave laser) loopback plug (Figure 5) is required to perform port diagnostic tests. Loopback plugs are shipped with the product, depending on the types of port transceivers installed.

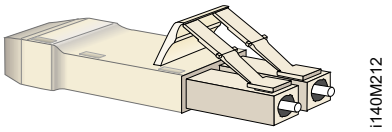


Figure 5 **Loopback plug**

- **Fiber-optic protective plug -** For safety and port transceiver protection, fiber-optic protective plugs (Figure 6) are inserted in all product ports without fiber-optic cables attached. Products are shipped with protective plugs installed.

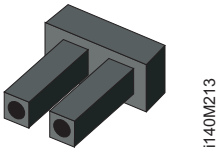


Figure 6 **Fiber-optic protective plug**

- **Null modem cable -** An asynchronous RS-232 null modem cable (Figure 7) is required to configure product network addresses and acquire event log information through the product's serial port. The cable has nine conductors and DB-9 female connectors.

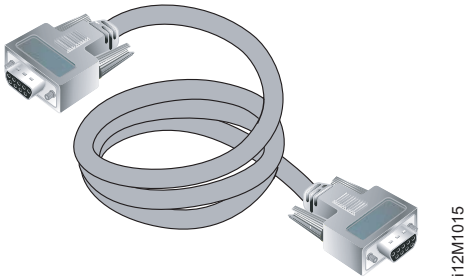


Figure 7 Null modem cable

Tools supplied by service personnel

The following tools should be supplied by service personnel:

- **Scissors or pocket knife -** A sharp cutting edge (scissors or knife blade) is required to cut protective strapping when unpacking replacement CRUs.
- **Flat-tip and cross-tip (Phillips) screwdrivers -** Screwdrivers are required to remove, replace, adjust, or tighten CRUs, chassis, or cabinet components.
- **T10 Torx® tool -** The tool is required to rack-mount products or to remove, replace, adjust, or tighten chassis or cabinet components.
- **ESD grounding cable and wrist strap -** An ESD wrist strap is required when working with ESD-sensitive CRUs, including optical transceivers.
- **Maintenance terminal -** A desktop or notebook PC is required to configure product network addresses and acquire event log information through the maintenance port. The PC must have:
  - The Microsoft® Windows® 98, Windows® 2000, Windows® 2003, Windows® XP, or Windows® ME operating system installed.
  - RS-232 serial communication software (such as ProComm Plus™ or HyperTerminal) installed. HyperTerminal is provided with Windows operating systems.
- **Fiber-optic cleaning kit -** The kit contains tools and instructions to clean fiber-optic cables, connectors, loopback plugs, and protective plugs.

Chapter 2: Installation tasks

This chapter describes tasks to install, configure, and verify operation of the SAN32M-2 using the,

- EFCM Basic Edition interface
- Storage area network (SAN) management application.
- Element Manager

The product can be installed on a table top, mounted in a 19-inch equipment rack.

Factory defaults

Table 2 lists factory-set defaults for the product.

Table 2 Factory-set defaults (product)

Item	Default
EFCM Basic Edition interface user name (case sensitive)	Administrator
EFCM Basic Edition interface password (case sensitive)	password
Customer-level password (maintenance port access)	password
Maintenance-level password (maintenance port access)	level-2
IP address	10.1.1.10
Subnet mask	255.0.0.0
Gateway address	0.0.0.0

Installation task summary

Table 3 summarizes installation tasks for the product, optional management server, and optional Ethernet hub. The table describes each task, states if the task is optional, and lists the page reference.

© Copyright IBM Corp. 2006

Table 3 Installation task summary

Task number and description	Required or optional	Page
Task 1: Verify installation requirements	Required.	19
Task 2: Unpack, inspect, and install the Ethernet hub (optional)	Perform task if hub is required to connect switch and management interface.	20
Task 3: Unpack, inspect, and install the product	Required.	24
Task 4: Configure product using EFCM Basic (optional)	Perform task if switch is managed through the EFCM Basic Edition interface.	27
Task 5: Configure product network information (optional)	Configure if connecting multiple switches or connecting switch and management server to a public LAN.	47
Task 6: Configure server password and network addresses	Required if management server is used.	50
Task 7: Configure management server information	Required if management server is used.	53
Task 8: Configure Windows operating system users	Required if management server is used.	56
Task 9: Set management server date and time	Required if management server is used.	59
Task 10: Configure the call-home feature (optional)	Configure if specified by customer and telephone connection is provided.	61
Task 11: Assign user names and passwords	Required if management server is used.	62
Task 12: Configure the product to the management application	Required if management server is used.	64
Task 13: Record or verify server restore information	Required if management server is used.	65
Task 14: Verify product-to-server communication	Required if management server is used.	66
Task 15: Configure PFE key (optional)	Configure if product feature enablement (PFE) key is ordered.	68
Task 16: Configure management server (optional)	Configure for open-systems host control of switch.	70
Task 17: Set product date and time	Required if management server is used.	72
Task 18: Configure the Element Manager application	Required if management server is used.	74
Task 19: Back up configuration data	Required if management server is used.	91
Task 20: Cable Fibre Channel ports	Required.	94
Task 21: Configure zoning (optional)	Perform task to configure zoning.	95
Task 22: Connect product to a fabric element (eptional)	Perform task to connect switch to a Fibre channel fabric.	96

Task 1: Verify installation requirements

Ensure that the following requirements are met prior to product and management interface installation.

- A site plan is prepared, configuration planning tasks are complete, planning considerations are evaluated, and related planning checklists are complete. Refer to the *IBM TotalStorage Products in a SAN Environment - Planning Manual* (GC26-7675) for information.
- Fibre Channel SAN design and director, switch, and SAN router device connectivity are evaluated, and the related planning worksheet is complete. Refer to the *IBM TotalStorage Products in a SAN Environment - Planning Manual* (GC26-7675) for information.
- Support is available for one of the following product management methods:
  - — A browser-capable PC and Internet connectivity to support the product-resident EFCM Basic Edition interface, *or*
  - — A rack-mount management server or browser-capable PC and LAN segment connectivity to support operation of SAN management and Element Manager applications.
- Support equipment and technical personnel are available for the installation.
- The required number and type of fiber-optic jumper cables are delivered and available. Ensure cables are the correct length and have the required connectors.
- An equipment cabinet or customer-supplied 19-inch equipment rack and associated hardware are available (optional).
- Remote workstations or simple network management protocol (SNMP) workstations are available (optional). Workstations are customer-supplied and connected through a public or dedicated LAN segment.

Task 2: Unpack, inspect, and install the Ethernet hub (optional)

The product is managed through either:

- An Internet connection to a browser-capable PC (EFCM Basic Edition interface): Connection of a LAN segment with multiple switches to the Internet may require installation of a 24-port Ethernet hub

or

- A 10/100 megabit per second (Mbps) LAN connection to a management server: Connectivity may require installation of a 24-port Ethernet hub. A combination of up to 48 products can be configured and managed on one network. Therefore, multiple, daisy-chained hubs may be required to provide sufficient port connections.

The following paragraphs provide instructions to unpack, inspect, and install one or more Ethernet hubs.

- If the existing Ethernet LAN segment is adequate for connectivity and a hub is not delivered, this task is not required. Go to *Task 3: Unpack, inspect, and install the product*.
- If the hub is delivered in an equipment cabinet, go to *Task 5: Configure product network information (optional)*.

Unpack and inspect Ethernet hub

Unpack and inspect Ethernet hub(s) as follows:

1. Inspect shipping container(s) for damage. Ensure that a freight carrier representative is present when the container is opened. Unpack shipping container(s) and inspect each item for damage. Ensure that the packaged items correspond to items listed on the enclosed bill of materials.
2. If any items are damaged or missing, within the United States and Canada, contact the IBM Quality Hotline toll-free 1-800-442-6773 or direct dial in other locations: 770-858-8459.

Desktop installation

To install and configure up to three Ethernet hubs on a desktop:

1. Remove the backing from the four adhesive rubber pads and apply the pads to the underside of each hub. Ensure that the pads are aligned with the scribed circles at each corner.
2. Position the first hub on a table or desktop as directed by the customer. Stack the remaining hubs on top of the first hub. Ensure that the adhesive rubber pads on the underside of a hub align with the recesses on the top of the hub below.
3. Daisy-chain (connect) the hubs:
   a. Connect the top and middle stacked hubs: Connect an RJ-45 patch cable to port **24** of the top hub, then connect the cable to port **12** of the middle hub.
   b. Connect the bottom and middle stacked hubs: Connect a second RJ-45 patch cable to port **24** of the middle hub, then connect the cable to port **12** of the bottom hub.
   c. Use a pointed instrument, Figure 8 (**1** and **2**), to set the medium-dependent interface (MDI) switch on the top and middle hubs to **MDI** (in). As shown in Figure 8 (**3**), set the MDI switch on the bottom hub to **MDIX** (out).

NOTE: To connect two hubs, use middle and bottom hub instructions only.

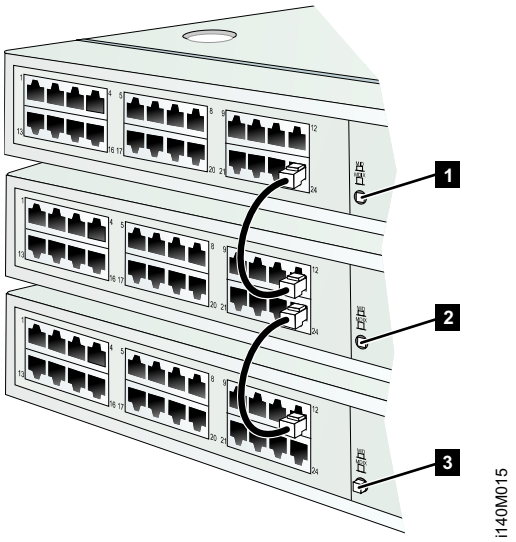


Figure 8 Patch cable and MDI selector configuration

4. Connect a power cord to an AC power strip and the receptacle at the rear of each hub. Use an extension cord if required.
5. Connect the AC power strip to facility power. Power for each hub switches on when the strip is connected to facility AC power.
6. Inspect the front panel of each hub. Ensure that each green **Power** light-emitting diode (LED) illuminates.

Rack-mount installation

You will need a pointed instrument (pencil tip or bent paper clip), #2 Phillips screwdriver, and 1/8-inch Allen wrench for this procedure.

To install and configure up to three Ethernet hubs in a SANC40M cabinet or customer-supplied 19-inch equipment rack, use the following steps:

1. Secure one mounting bracket to each side of the first hub as shown in Figure 9. Use the two brackets and four pan-head Phillips screws (8/32 x 0.5-inch) provided.

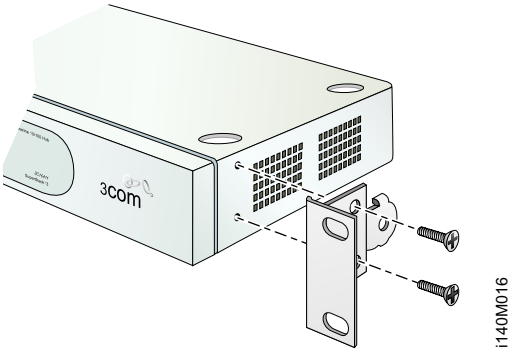


Figure 9 **Mounting bracket installation (Ethernet hub)**

2. Position the hub as directed by the customer. Align screw holes in the mounting brackets with screw holes in the rack-mount standards.
3. Secure both sides of the hub to the rack-mount standards. Use the 1/8-inch Allen wrench and four Allen-head mounting screws (10/32 x 0.5-inch) provided.
4. Repeat all previous steps in this procedure for the remaining hubs.
5. Daisy-chain (connect) the hubs:
   a. Connect the top and middle stacked hubs: Connect an RJ-45 patch cable to port **24** of the top hub, then connect the cable to port **12** of the middle hub.
   b. Connect the bottom and middle stacked hubs: Connect a second RJ-45 patch cable to port **24** of the middle hub, then connect the cable to port **12** of the bottom hub.
   c. Use a pointed instrument, as shown in *Patch cable and MDI selector configuration* (**1** and **2**), to set the medium-dependent interface (MDI) switch on the top and middle hubs to **MDI** (in). As shown in Figure 8 (**3**), set the MDI switch on the bottom hub to **MDIX** (out).

NOTE: To connect two hubs, use the middle and bottom hub instructions only.

6. Connect a power cord to a rack power strip and the receptacle at the rear of each hub. Power for each hub switches on when the hub (and equipment rack) are connected to facility AC power.

   NOTE: Ensure that each hub is connected to a separate rack power strip.

7. Inspect the front panel of each hub. Ensure each green **Power** LED illuminates.

Task 3: Unpack, inspect, and install the product

Follow the procedures in this section to unpack, inspect, and install the switch in a rack-mount configuration.

Unpack and inspect switch

Unpack and inspect the switch(es) as follows:

1. Inspect shipping container(s) for damage caused during transit. Ensure that a representative from the freight carrier is present when the container is opened.
2. Unpack shipping container(s) and inspect each item for damage. Ensure that the packaged items correspond to the items listed on the enclosed bill of materials.
3. If any items are damaged or missing, contact the IBM Quality Hotline toll-free at 1-800-442-6773 within the United States and Canada. In other locations direct dial 770-858-8459.

Desktop installation

To install a switch on a desktop:

1. Remove the backing from the four adhesive rubber pads and apply the pads to the underside of the switch. Ensure that the pads are aligned with the scribed circles at each corner.
2. Position the switch on a table or desktop as directed by the customer. Ensure that:
   - — Grounded AC electrical outlets are available.
   - — Adequate ventilation is present, and areas with excessive heat, dust, or moisture are avoided.

— All planning considerations are met. Refer to *IBM TotalStorage Products in a SAN Environment - Planning Manual* (GC26-7675) for information.

3. Ensure that all customer-replaceable units (CRUs) are installed as ordered.
4. Connect both AC power cords to receptacles at the rear of the chassis.
5. Connect AC power cords to separate (for redundancy) facility power sources that provide single-phase, 100 to 240 volt alternating current (VAC) current.

   The switch powers on and performs power-on self-tests (POSTs). During POSTs:

   a. The green power (**PWR**) LED on the front panel illuminates.
   b. The amber system error (**ERR**) LED on the front panel blinks momentarily while the switch is tested.
   c. The green LED associated with the Ethernet port blinks momentarily while the port is tested.
   d. LEDs associated with Fibre Channel ports blink momentarily while the ports are tested.

   After successful POST completion, the **PWR** LED remains illuminated and all other front panel LEDs extinguish.

   If a POST error or other malfunction occurs, go to *MAP 0000: Start MAP* to isolate the problem.
6. Perform one of the following:

   — If the switch is to be managed through the EFCM Basic Edition interface, go to *Task 4: Configure product using EFCM Basic (optional)*.

   — If the switch is to be managed through a management or customer-supplied server, go to *Task 5: Configure product network information (optional)*.

Rack-mount installation

Perform the following steps to install and configure the switch in an equipment cabinet or a customer-supplied equipment rack. An optional rack-mount kit, T10 Torx tool, and #2 Phillips screwdriver are required.

1. Locate the rack-mount position as directed by the customer.
2. Ensure that all CRUs are installed as ordered.
3. Open the rack-mount kit and inspect the contents. Refer to the enclosed bill of materials and ensure that all parts are delivered.
4. Using a T10 Torx tool and #2 Phillips screwdriver, install the switch in the equipment cabinet.
5. Connect both AC power cords to receptacles at the rear of the chassis.
6. Connect AC power cords to separate (for redundancy) rack power strips connected to a facility power source that provides single-phase, 100 to 240 VAC current.

   When the first power cord is connected, the switch powers on and performs POSTs. During POSTs:

   a. The green power (**PWR**) LED on the front panel illuminates.
   b. The amber system error (**ERR**) LED on the front panel blinks momentarily while the switch is tested.
   c. The green LED associated with the Ethernet port blinks momentarily while the port is tested.
   d. LEDs associated with Fibre Channel ports blink momentarily while the ports are tested.

   After successful POST completion, the **PWR** LED remains illuminated and all other front panel LEDs extinguish.

   If a POST error or other malfunction occurs, go to *MAP 0000: Start MAP* to isolate the problem.
7. Perform one of the following:

   — If the switch is to be managed through the EFCM Basic Edition interface, go to *Task 4: Configure product using EFCM Basic (optional)*.

   — If the switch is to be managed through a management or customer-supplied server, go to *Task 5: Configure product network information (optional)*.

Task 4: Configure product using EFCM Basic (optional)

Perform these procedures to configure the product from the EFCM Basic Edition interface. A browser-capable PC with Internet or Ethernet LAN access is required. To open the interface:

1. Connect the Ethernet patch cable (supplied with the product) to the RJ-45 connector (labelled **10/100**) at the front panel.
2. Connect the remaining end of the Ethernet cable to the Internet or LAN segment as directed by the customer. If the hub installed in *Task 2: Unpack, inspect, and install the Ethernet hub (optional)* provides connectivity, connect the cable to any available hub port.
3. Launch the browser application (Netscape Navigator or Internet Explorer) on the PC.
4. Enter the default Internet Protocol (IP) address of the switch (**10.1.1.10**) as the uniform resource locator (URL). The *Enter Network Password* dialog box appears.
5. Type the case-sensitive default user name (**Administrator**) and password (**password**) and click *OK*. The *First Time Login* view appears.
6. Type customer-specified values in the *User Name*, *New Password*, and *Confirm Password* fields, then click *Activate*. The *Topology* view appears with status information about each fabric element, including the product to be configured.
7. Click *Switch Details*. The *Hardware* view appears (Figure 10).

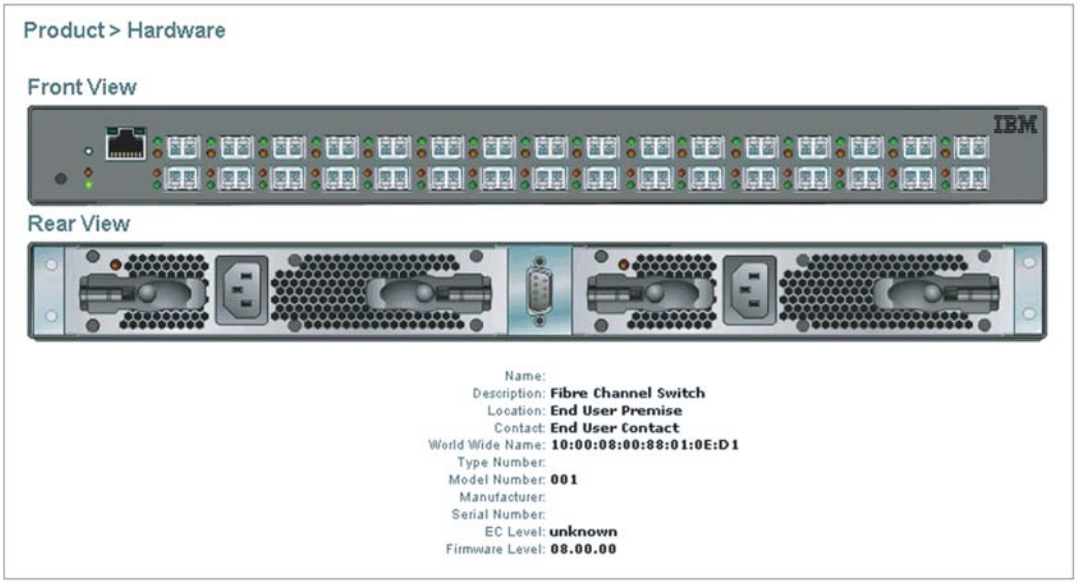


Figure 10 Hardware View

8. Configure the product from the EFCM Basic Edition interface by selectively performing the following tasks according to customer requirements:

Product	• Identification • Date and time • Parameters • Fabric parameters • Network addresses.
Ports	• Basic information • Buffer-to-buffer credits (BB_Credits) • N_Port identifier virtualization (NPIV).
Management	• SNMP trap message recipients • Command line interface (CLI) • Open systems management server (OSMS) • Secure socket layer (SSL) encryption.

Options	Product feature enablement (PFE) keys.
Security	• SANtegrity authentication (settings, access control list, and remote authentication dial-in user service (RADIUS) server support), • Enterprise Fabric Mode • SANtegrity binding (fabric, switch, and port binding
Interswitch Links	• OpenTrunking • Preferred path, and • Interswitch link (ISL) port fencing

Configure product identification

Perform this procedure to configure the product identification.

NOTE: The *Name*, *Location*, and *Contact* variables correspond respectively to the SNMP variables *sysName*, *sysLocation*, and *sysContact*, and are used by management workstations when obtaining product data.

1. Select *Identification* from the *Configure* menu (*Configure>Switch>Identification*). The *Identification* view appears (Figure 11).

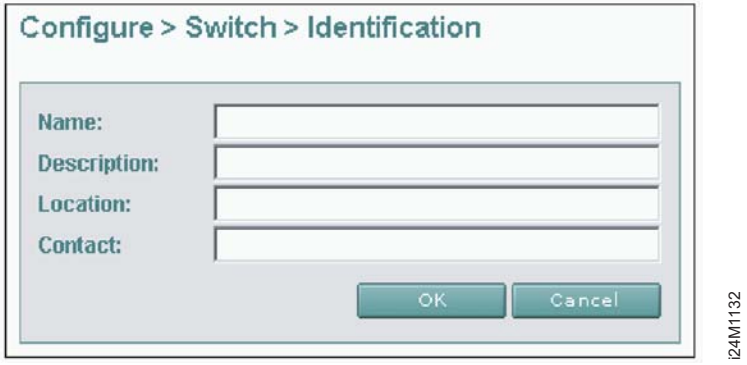


Figure 11 Identification View

a. Type a unique product name (less than 24 alphanumeric characters) in the *Name* field. If installed on a public LAN, the name should reflect the product's Ethernet network domain name system (DNS) host name.

b. Type a product description (less than 255 alphanumeric characters) in the *Description* field.

c. Type the product's physical location (less than 255 alphanumeric characters) in the *Location* field.

d. Type the name of a contact person (less than 255 alphanumeric characters) in the *Contact* field.

2. Click *OK* to save and activate changes.

Configure date and time

To configure the product date and time, use the following steps:

1. Select *Date & Time* from the *Configure* menu (*Configure>Switch>Date & Time*). The *Date Time* view appears (Figure 12).

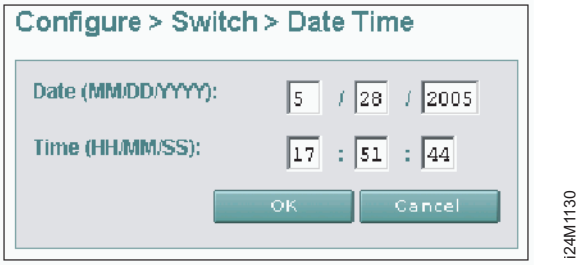


Figure 12 Date Time View

a. Configure the Date using the *Date* field:

- Month (*MM*): **1** - **12**.
- Day (*DD*): **1** - **31**.
- Year (*YYYY*): greater than **1980**.

b. Configure the Time using the *Time* field:

- Hour (*HH*): **0** - **23**.
- Minute (*MM*): **0** - **59**.
- Second (*SS*): **0** - **59**.

2. Click *OK* to save and activate changes.

Configure parameters

To configure product operating parameters, use the following steps:

1. Set the product offline. Refer to *Set online state* for instructions.
2. Select *Parameters* from the *Configure* menu (*Configure>Switch>Parameters*). The *Parameters* view appears (Figure 13).
   a. Select the *Domain ID Offset* value from the drop-down list. Values available in the drop-down list are 0, 32, 64, 96 (default), 128, 160, and 192. Domain IDs minus the offset are still in the 1-31 range.

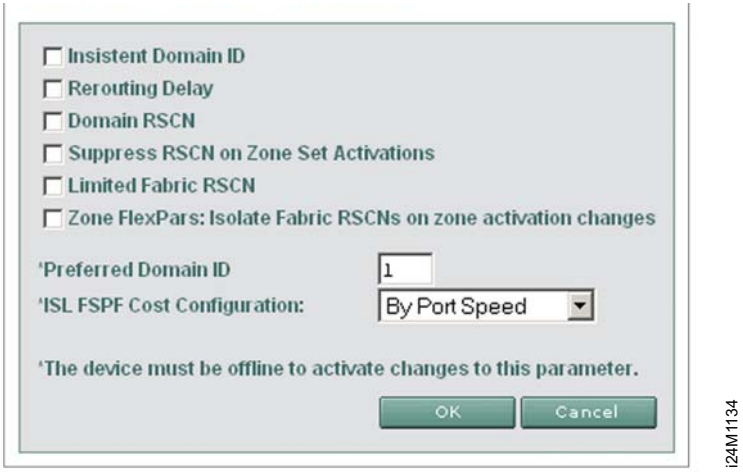


Figure 13 Parameters View

   b. Type a value (1-31) in the *Preferred Domain ID* field.
   c. Enable (check) the *Insistent Domain ID* field if you want the *Preferred Domain ID* to become the active domain ID when the fabric initializes.
   d. Enable (check) the *Rerouting Delay* field if you want the traffic to be delayed through the fabric by the error detect time out value (E_D_TOV). This delay ensures that the Fibre Channel frames are delivered to their destination in order.

e. Enable (check) the *Domain RSCN* field, if you want the attached devices to register and receive notification when other devices change state.

f. Enable (check) the *Suppress RSCN on Zone Set Activations* if you do not want the RSCNs to be transmitted when a zone set is activated.

g. Enable (check) the *Isolate on zone activations* field if you want only devices that require RSCN notification due to a zoning configuration change to receive RSCNs. Do not enable this option if *Suppress on zone set activations* is enabled because RSCNs will not be sent to attached devices.

h. Enable (check) the *Limited Fabric RSCN* field if you do not want the RSCNs to be transmitted after a switch initial program load (IPL).

3. Click *OK* to save and activate changes.
4. Set the product online. Refer to *Set online state* for instructions.

Configure fabric parameters

To configure fabric operating parameters, use the following steps:

1. Set the product offline. Refer to *Set online state* for instructions.
2. Select *Fabric Parameters* from the *Configure* menu (*Configure>Switch>Fabric Parameters*). The *Fabric Parameters* view appears (Figure 14).

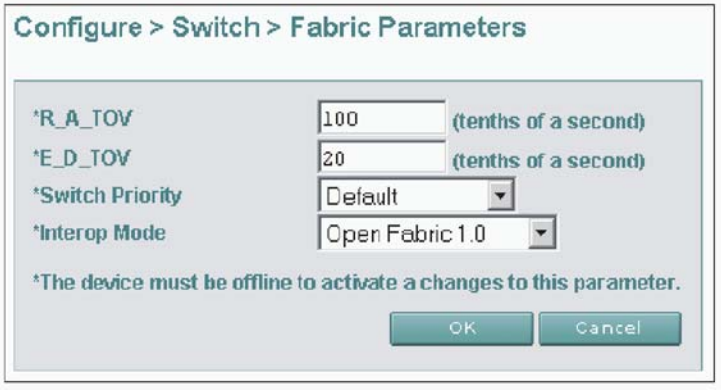


Figure 14 Fabric Parameters View

a. Type a value between **10 - 1200** tenths of a second (1 - 120 seconds) in the *R_A_TOV* field. Ten seconds (**100**) is the recommended value. The R_A_TOV value must exceed the E_D_TOV value.

b. Type a value between **2 - 600** tenths of a second (0.2 - 60 seconds) at the *E_D_TOV* field. Two seconds (**20**) is the recommended value.

NOTE: Fabric elements must be set to the same R_A_TOV and E_D_TOV values. An ISL between fabric elements with different values segments and prevents communication.

---

c. Select from the *Switch Priority* drop-down list to designate the fabric's principal switch. The principal switch is assigned a priority of **1** and controls the allocation and distribution of domain IDs for all fabric elements (including itself). Available selections are *Default*, *Principal*, and *Never Principal*.

Principal is the highest priority setting, *Default* is next, and *Never Principal* is the lowest. At least one switch in a fabric must be set as *Principal* or *Default*. If all switches are set to *Never Principal*, all ISLs segment.

d. Select from the *Interop Mode* drop-down list to set the product operating mode. This setting affects the management mode and does not affect port operation. The available selections are:

- **McDATA Fabric 1.0 -** Select this option if the product is fabric-attached only to other IBM directors or switches operating in McDATA fabric mode.
- **Open Fabric 1.0 -** Select this option (default) for managing heterogeneous fabrics and if the product is fabric-attached to IBM directors or switches and other open-fabric compliant switches.

NOTE: With Open Fabric 1.0 enabled, the default zone set is disabled.

---

3. Click *OK* to save and activate changes.
4. Set the product online. Refer to *Set online state* for instructions.

Configure network information

Follow the procedure in this section to configure the network information.

Ensure the LAN installation with the network administrator.

- If only one product is installed on a dedicated LAN, network information (IP address, subnet mask, and gateway address) does not require change.
- If multiple products are installed or a public LAN segment is used, network information must be changed to conform to the LAN addressing scheme.

To change the product network information, use the following steps:

1. Select *Network* from the *Configure* menu (*Configure>Switch>Network*). The *Network* view appears (Figure 15).

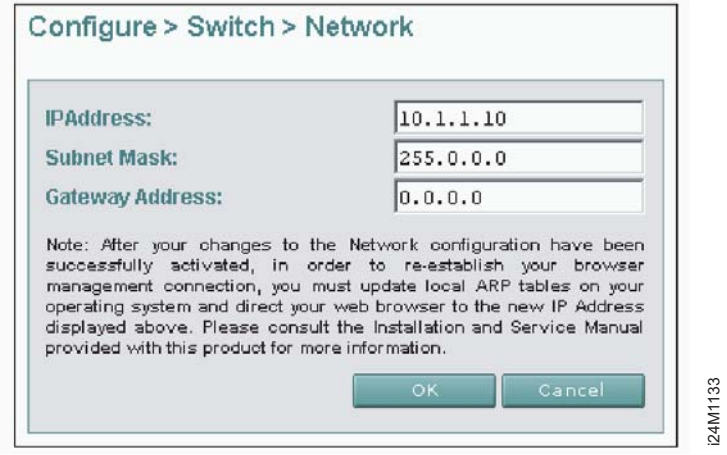

Configure > Switch > Network
IPAddress:
10.1.1.10
Subnet Mask:
255.0.0.0
Gateway Address:
0.0.0.0
Note: After your changes to the Network configuration have been successfully activated, in order to re-establish your browser management connection, you must update local ARP tables on your operating system and direct your web browser to the new IP Address displayed above. Please consult the Installation and Service Manual provided with this product for more information.
OK
Cancel
i24M1133

Figure 15 Network View

   a. Type a value in the *IP Address* field (default is **10.1.1.10**).

   b. Type a value in the *Subnet Mask* field (default is **255.0.0.0**).

   c. Type a value in the *Gateway Address* field (default is **0.0.0.0**).

2. Click *OK* to save and activate changes.

   An acknowledgement message appears, indicating that the browser PC must be directed to the new IP address.

3. Update the address resolution protocol (ARP) table for the browser PC.
    a. Close the EFCM Basic Edition interface and all browser applications.
    b. Open the command prompt (DOS) on your Windows desktop.
    c. Delete the switch's ***old*** IP address from the ARP table. At the command (**C:**) prompt, type **arp -d** ***xxx.xxx.xxx.xxx***, where ***xxx.xxx.xxx.xxx*** is the old IP address for the switch.
    d. Close the command prompt window and return to the Windows desktop.
4. Perform a power-on reset (POR) (*IML or reset switch*).
5. Open the browser (Internet Explorer or Netscape Navigator) on your PC. Enter the ***new*** IP address of the product as the URL. The *Enter Network Password* dialog box appears.
6. Type the case-sensitive user name and password and click *OK*. The *EFCM Basic Edition* interface appears with the *Topology* view displaying the status information of each fabric element.

Configure basic port information

To configure basic port information, use the following steps:

1. Select *Basic Info* from the *Configure* menu (*Configure>Ports>Basic Info*). The *Basic Information* view appears(Figure 16).
    a. Type a port name (24 alphanumeric characters or less) for each port to be configured in the *Name* field. The port name should characterize the device to which the port is attached.
    b. Enable the check box in the *Blocked* column if you want to block a port (default is unblocked).
    c. Disable the check box in the *Fabric Address Notify* column if you want to disable the feature (default is enabled). When enabled, an FL_Port transmits FAN frames after loop initialization to ensure that FC-AL devices are still logged in.

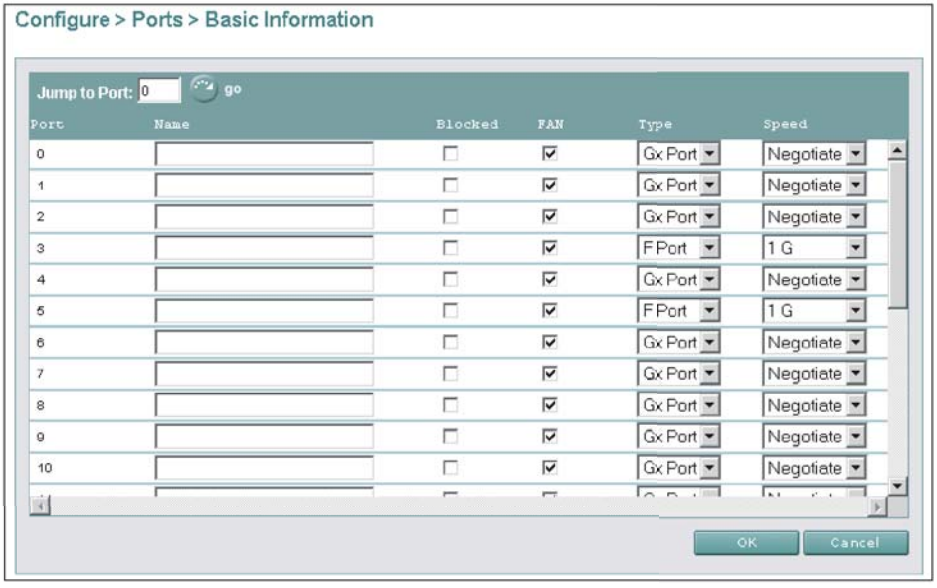


Figure 16 Basic Information View

d. Select from the drop-down list in the *Type* column to configure the port type. The available options are fabric port (**F_Port**), expansion port (**E_Port**), generic port (**G_Port**), generic mixed port (**GX_Port**), and fabric mixed port (**FX_Port**).

e. Select from the drop-down list in the *Speed* column to configure the port transmission rate. The available options are auto-negotiate between 1.0625 and 2.1250 Gbps operation (**Negotiate**), 1.0625 Gbps operation (**1 Gb/sec**), 2.1250 Gbps operation(**2 Gb/sec**), and 4.2500 Gbps operation (**4 Gb/sec**).

2. Click *OK* to save and activate changes.

Configure port BB_Credit

Follow the procedure in this section to configure a port to receive BB_Credits.

The switch provides two port buffer pools of 235 receive BB_Credits each (470 credits total). Ports **0** through **3**, **8** through **11**, **16** through **19**, and **24** through **27** share buffer pool zero. Ports **4** through **7**, **12** through **15**, **20** through **23**, and **28** through **31** share buffer pool one. Each port can be assigned between two and 120 credits, provided the

total credits allocated to all ports in a pool does not exceed 235. The default value is 12 credits per port.

To configure a port to receive BB_Credits, use the following steps:

1. Set all (or a subset of user-specified) ports offline. Refer to *Set online state* or *Block or unblock a port* for instructions.
2. Select *RX BB Credit* from the *Configure* menu (*Configure>Ports>RX BB Credit*). The *RX BB Credit* view appears.
3. Perform one of the following:
   - To set all offline ports to default values, click *Default*.
   - To set an offline port to a user-specified value, type the desired value in the *RX BB Credit* column.
4. Click *OK* to save and activate changes.
5. Set all or user-specified ports online. Refer to *Set online state* (all) or *Block or unblock a port* (specified ports) for instructions.

Configure port NPIV

NPIV allows multiple (up to 256) Fibre Channel addresses to be assigned to a node (N_Port). The NPIV feature must be installed. Refer to *Install PFE keys (optional)* for instructions.

To configure ports for NPIV connectivity, use the following steps:

1. Select *NPIV* from the *Configure* menu (*Configure>Ports>NPIV*). The *NPIV* view appears.
2. Click *Enable* to activate NPIV operation for the product.
3. Type a desired value (**1 - 256**) in the *Login* column.
4. Click *OK* to save and activate changes.

Configure SNMP

Follow the procedure in this section to configure names, write authorizations, addresses, and user datagram protocol (UDP) port numbers for SNMP trap message recipients.

To configure recipient workstations, use the following steps:

1. Select *SNMP* from the *Configure* menu (*Configure>SNMP*). The *SNMP* view appears (Figure 17).

a. Click *Enable* to activate the installed SNMP agent.

b. Select the appropriate Fibre Alliance management information base (FA MIB) from the *FA MIB Version* drop-down list. Valid selections are **FA MIB Version 3.0** or **FA MIB Version 3.1**.

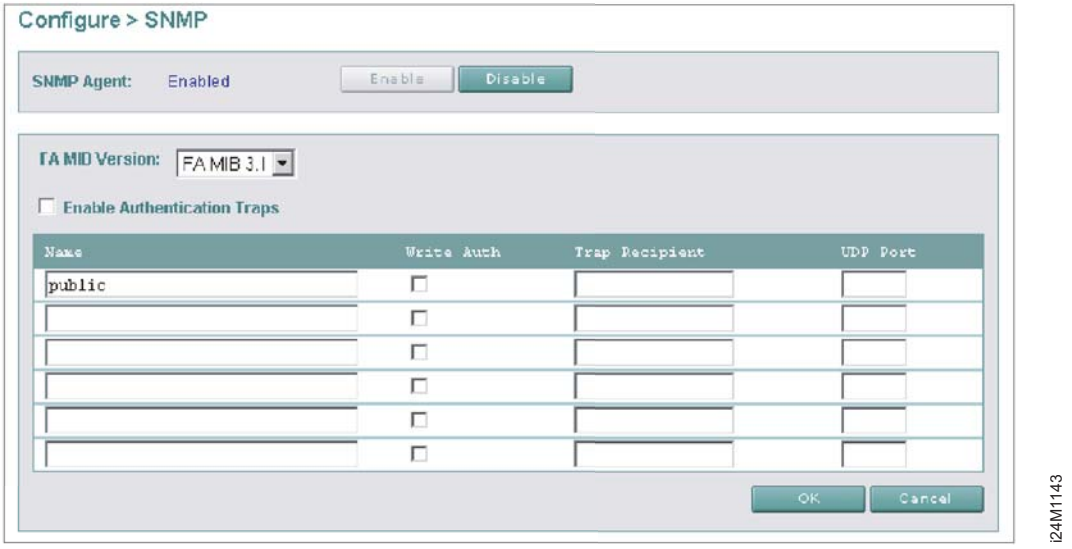


Figure 17 SNMP View

c. Select (check) the *Enable Authentication Traps* check box to enable transmission of SNMP trap messages to recipients.

d. Type a community name for each configured recipient (less than 32 alphanumeric characters) in the *Name* field. The name is incorporated in SNMP trap messages to prevent unauthorized viewing.

e. Check the box in the *Write Auth* column if you want to enable write authorization for the trap recipient (default is disabled). When enabled, a configured user can change *sysContact*, *sysName*, and *sysLocation* SNMP variables.

f. Type the IP address or DNS host name of the trap recipient (SNMP management workstation) in the *Trap Recipient* field. It is recommended that the IP address be used.

g. Type a decimal port number in the *UDP Port Number* field to specify the UDP port number

2. Click *OK* to save and activate changes.

Enable CLI

Follow the procedure in this section to toggle (enable or disable) the state of the product's command line interface (CLI).

To change the CLI state, use the following steps:

1. Select *CLI* from the *Configure* menu. The *CLI* view appears (Figure 18).

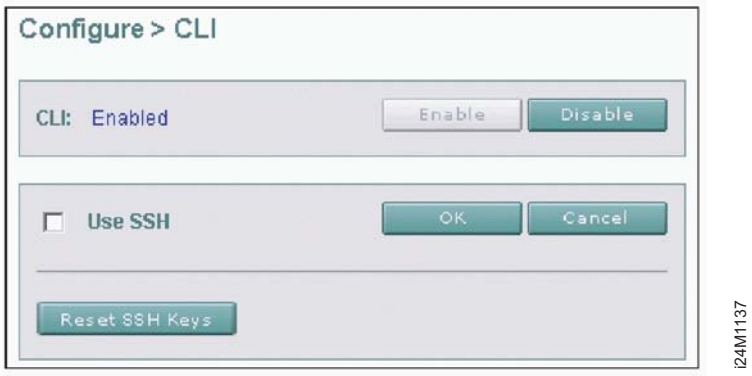


Figure 18 CLI View

2. Perform one of the following:
   - Click *Enable* to activate the CLI.
   - Click *Disable* to deactivate the CLI.
3. Click (check) the *Use SSH* check box to enable secure shell (SSH) protocol. The protocol controls CLI access to the product and provides software-enforced encryption.
4. Click *OK* to save and activate changes.

Enable or disable host control

Follow the procedure in this section to configure the open systems management server and enable OSI host control of the product. Implementing and enabling OSI host control requires installation of a SAN management application on the OSI server. Applications include Veritas® SANPoint™ Control or Tivoli® NetView®.

To enable or disable OSMS host control, use the following steps:

Open Systems Only

1. Select *OSMS* from the *Configure* menu. The *OSMS* view appears (Figure 19).

Figure 19 OSMS View

2. Perform one of the following:
   - Click *Enable* to activate OSMS.
   - Click *Disable* to deactivate OSMS.
3. Click (check) the *Enable Host Control* check box to activate host control of the product.
4. Click *OK* to save and activate changes.

Configure SSL encryption

SSL is a protocol that encrypts internet communications. The protocol uses key encryption and includes a digital certificate that enables server authentication and SSL session initialization.

When *web SSL* is enabled, all data transmitted over an authenticated internet connection is encrypted.

Software SSL enables use of an application program interface (API) connection. With software SSL enabled, secure and unsecure communications are acceptable, however, unsecure communications are directed to an encrypted API connection.

An SSL session key (not part of the digital certificate) is valid only during the SSL connection, and is renegotiated as per the value entered. The *Renegotiate After* value defines the amount of data (in MB) that may be transmitted over the connection before triggering the regeneration of a new SSL session key.

To configure SSL encryption, use the following steps:

1. Select *SSL* from the *Configure* menu (*Configure>SSL*). The *SSL* view appears (Figure 20).
2. Do one of the following:
   - Click *Enable* to activate web SSL.
   - Click *Disable* to deactivate web SSL.
3. Do one of the following:
   - Click *Enable* to activate software SSL.
   - Click *Disable* to deactivate software SSL.

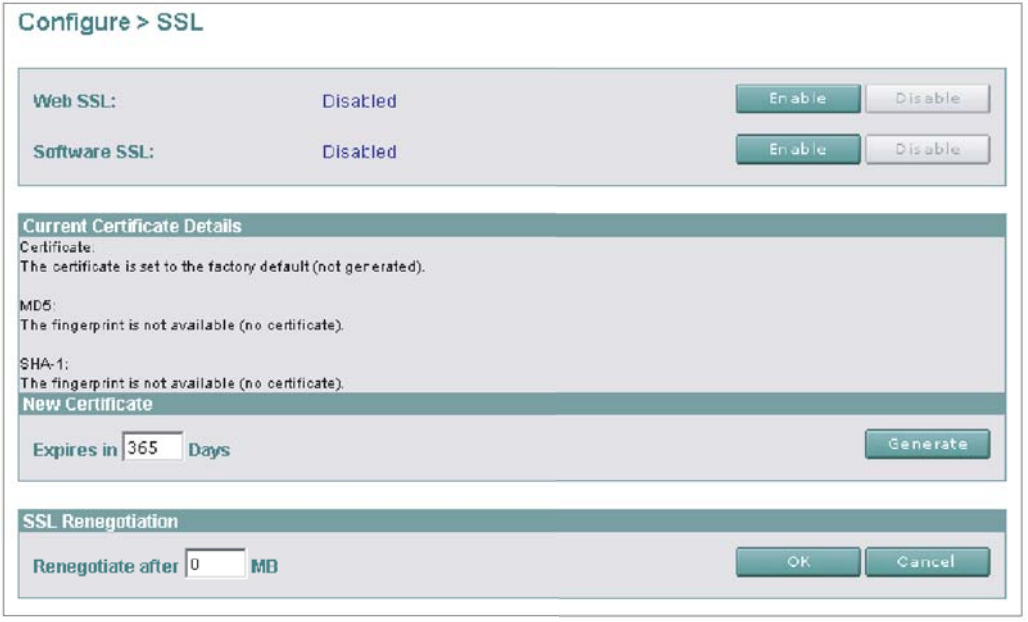


Figure 20 SSL View

4. Type a value between **30** and **3650** in the *Expires in* field to define the expiration period (in days) of the digital certificate. The default is **365** days.
5. Click *Generate* to generate a new certificate.

6. Type a value between **50** and **10000** in the *Renegotiate after* field to define a renegotiation parameter (in megabytes) for the SSL session key.
7. Click *OK* to save and activate changes.

Install PFE keys (optional)

Follow the procedures in this section to install optional features using PFE keys.

After purchasing a feature, obtain the PFE key by following the enclosed instructions. The key is an alphanumeric string consisting of uppercase and lowercase characters that must be entered exactly, including dashes. An example format is:

XxXx-XXxX-xxXX-xX.

NOTE: PFE keys are encoded to work with the serial number of the installed switch only. Record the key to re-install the feature if required. If the switch fails and must be replaced, obtain new PFE keys from IBM. Please have the serial numbers of the failed and replacement switches, and the old PFE key number or transaction code.

The optional features you can install using PFE-keys are listed below:

- **Element Manager application -** This feature enables out-of-band product management through an Element Manager interface. Products are delivered with the application enabled for a 31-day grace period. Before grace period expiration, the application must be reactivated through a PFE key.
- **FICON management server -** These feature supports inband product management through FMS host control.
- **Flexport Technology** - A Flexport Technology product is delivered at a discount with all Fibre Channel ports disabled. When additional port capacity is required, the remaining ports are incrementally enabled through this feature.
- **Full volatility -** This feature ensures no Fibre Channel frames are stored after the product is powered off or fails, and a memory dump file (that possibly includes classified data frames) is not included as part of the data collection procedure.
- **N_Port ID virtualization -** This feature allows up to 256 Fibre Channel addresses to be assigned to an N_Port.

- **SANtegrity binding -** This feature enhances security in SANs with a large and mixed group of fabrics and attached devices.
- **SANtegrity authentication -** This feature enhances security of the product by controlling the ability of users, devices, and processes to attach to the product.
- **OpenTrunking -** This feature provides dynamic load balancing of Fibre Channel traffic across multiple ISLs.

To, install the optional features using EFCM Basic, use the following steps:

1. Select *Optional Features* from the *Configure* menu (*Configure*>*Optional Features*) ***or*** *Security* menu (*Security*>*Optional Features*). The *Maintenance Feature Installation* view appears (Figure 21).

   The installed features are denoted by a green check mark (installed) and features that have not been installed or uninstalled are denoted by a red cross mark. Flexport Technology status is indicated by the number of installed ports.

   For the description of a feature, click the feature title in the *Feature* panel. A description is displayed in the *Feature Details* panel.

Maintenance Feature Installation
Serial Number: TEST
Feature Key:
Update
Feature
Installed
Feature Details
Element Manager
Flex Ports
0
Full Volatility
N_port ID Virtualization
SANtegrity Binding
SANtegrity Authentication
Open Trunking
SANtegrity Binding
Binding is a set of features that locks a fabric into an intended configuration. Binding defends against malicious threats such as WWN spoofing for N Ports and E Ports as well as enabling two-factor change management processes that improve system stability by locking out physical changes until they are authorized.
Contact Sales at 1-800-545-5773
OK
Cancel
Disable Feature Information
i24M1147

Figure 21 Maintenance Feature Installation View

2. Type the key in the *Feature Key* field and click *Update*. The interface refreshes and indicates the update changes in the *Feature* panel.

NOTE: When *OK* is selected, all features are updated with new features.

3. Click *OK*.

   The new PFE key(s) are activated, the message **Feature installation in process. Your browser connection will be unavailable until unit restart is complete** is displayed, and the product performs a non-disruptive (to Fibre Channel traffic) firmware reset.

   After the product reset, the message **Feature installation complete. Click here to login.** is displayed.

4. Login and start a new EFCM Basic Edition session. The *Enter Network Password* dialog box appears.

Configure security

This section describes optional product security features configured through *Security* menu selections. The enhanced SANtegrity PFE key must be installed. Refer to *Install PFE keys (optional)* for instructions.

Select *Security* and choose from one of the following options in the drop-down menu.

- **Authentication settings -** Use the *Authentication Settings* view (*Security>Authentication Settings*) to configure the optional SANtegrity authentication features, including:
  - **User settings -** Use this page to configure the password-protected administrator and operator access to the EFCM Basic Edition and command line interfaces.
  - **Software settings -** Use this page to configure challenge handshake authentication protocol (CHAP) controlled management interface access (out-of-band and inband) to the product.
  - **Device settings -** Use this page to configure a CHAP secret authentication sequence for nodes (devices) attached to the product through E_Ports or N_ports.
  - **Port settings -** Use this page to override product-level authentication settings and enable or disable device communication on a per-port basis.
- **IP access control list -** Use the *IP Access Control List* view (*Security>IP Access Control List*) settings to configure a list of device IP addresses or a range of device IP addresses that are authorized to communicate with the product.

- **RADIUS -** Use the *RADIUS Server* view (*Security>RADIUS*) to configure up to three remote authentication dial-in user service (RADIUS) servers. A RADIUS server stores and authenticates passwords and CHAP secrets.
- **Enterprise Fabric Mode -** Use the *Enterprise Fabric Mode* view (*Security>Enterprise Fabric Mode*) to enable or disable Enterprise Fabric Mode (EFM). Fabric binding is activated when EFM is enabled.
- **Fabric binding -** Use the *Fabric Binding* view (*Security>Fabric Binding*) to lock parameters of a fabric in accordance with the user configuration. Fabric binding creates a membership list of element (director or switch) Domain_IDs and worldwide names (WWNs) that can communicate with the product.
- **Switch binding -** Use the *Switch Binding* view (*Security>Switch Binding*) to create a membership list of node (device) WWNs that can attach to the product. The specified connection policy restricts product access through E_Ports, F_Ports, or in general (all ports).
- **Port binding -** Use the *Port Binding* view (*Security>Port Binding*) to bind an attached device WWN to a product Fibre Channel port.

To configure optional features, refer to the *EFCM Basic Edition User Manual* (620-000240) for instructions.

Configure interswitch links

This section describes optional ISL performance features configured through *Configure* menu selections.

The ISL performance features include:

- **Open Trunking -** You can select *OpenTrunking* from the *Configure* menu (*Configure>Performance>Open Trunking*). Use the *Open Trunking* view to optimize ISL bandwidth. The feature monitors data rates (congestion and BB_Credit starvation) through multiple ISLs and load balances traffic (from congested to uncongested links) accordingly.
- **Preferred path -** You can select *Preferred Path* from the *Configure* menu (*Configure>Performance>Preferred Path*). Use the *Preferred Path* view to specify and configure one or more ISL data paths between multiple fabric elements. At each fabric element, a preferred path consists of a source port, exit port, and destination Domain_ID.

- **Port fencing -** You can select *Port Fencing* from the *Configure* menu (*Configure>Port Fencing*). Use the *Port Fencing* view to minimize ISLs that bounce (repeatedly attempt to establish a connection), causing disruptive fabric rebuilds. Fencing defines a bounce threshold that when reached, automatically blocks the disruptive E_Port.

To configure optional features, refer to the *EFCM Basic Edition User Manual* (620-000240) for instructions.

If no additional options or features are to be configured, skip to *Task 20: Cable Fibre Channel ports*.

Task 5: Configure product network information (optional)

The product is delivered with default network addresses as follows:

- **MAC address -** The media access control (MAC) address is programmed into FLASH memory on the control processor (CTP) card at manufacture. The MAC address is unique for each product, and should not be changed.
- **IP address -** The default IP address is **10.1.1.10**. If multiple products are installed on the same LAN, each product (and the management server) must have a unique IP address.

  NOTE: If multiple products and the management server are delivered in an equipment cabinet, all devices are configured with unique IP addresses that do not require change. The addresses require change only if multiple cabinets are LAN-connected.

- **Subnet mask -** The default subnet mask is **255.0.0.0**. If the product is installed on a complex public LAN with one or more routers, the address may require change.
- **Gateway address -** The default gateway address is **0.0.0.0**. If the product is installed on a public LAN, the gateway address must be changed to the address of the corporate intranet's local router.

Ensure the LAN installation with the customer. If one product is installed on a dedicated LAN, network addresses do not require change. Skip to *Task 6: Configure server password and network addresses*.

If multiple products are installed or a public LAN segment is used, network addresses must be changed to conform to the customer's LAN addressing scheme.

Perform the following steps to change a product IP address, subnet mask, or gateway address.

NOTE: An asynchronous RS-232 modem cable and maintenance terminal (desktop or notebook PC) with a Windows-based operating system and RS-232 serial communication software (such as ProComm Plus or HyperTerminal) are required.

1. Remove the protective cap from the 9-pin maintenance port at the rear of the chassis, using a Phillips screwdriver. Connect one end of the RS-232 modem cable to the port.
2. Connect the other cable end to a 9-pin serial communication port (**COM1** or **COM2**) at the rear of the maintenance terminal PC.
3. Power on the maintenance terminal. At the Windows desktop, click *Start* at the left side of the task bar. The *Windows Workstation* menu appears.

   NOTE: The following steps describe changing network addresses using HyperTerminal serial communication software.

4. Open the *HyperTerminal* window on your *Windows Workstation* (*Start>Programs>Accessories>Communications>HyperTerminal*). The *Connection Description* dialog box appears (Figure 22).

Figure 22 Connection Description dialog box

5. Type a descriptive product name in the *Name* field and click *OK*. The *Connect To* dialog box appears.
6. Ensure that the *Connect using* field displays **COM1** or **COM2** (depending on the port connection to the product), and click *OK*. The *COMn Properties* dialog box appears, where *n* is **1** or **2**.
7. Configure *Port Settings* parameters:
   - *Bits per second* - **115200**.
   - *Data bits* - **8**.
   - *Parity* - **None**.
   - *Stop bits* - **1**.
   - *Flow control* - **Hardware** or **None**.

   Click *OK*. The *New Connection - HyperTerminal* window appears.
8. Type the user password (default is **password**) at the **>** prompt, and press **Enter**. The password is case sensitive. The *New Connection - HyperTerminal* window appears with software and hardware version information for the product, and a **C >** prompt at the bottom of the window.
9. Type the **ipconfig** command at the **C >** prompt, and press the **Enter** key. The *New Connection - HyperTerminal* window appears with the following configuration information:
   - *MAC Address*.
   - *IP Address* (default is **10.1.1.10**).
   - *Subnet Mask* (default is **255.0.0.0**).
   - *Gateway Address* (default is **0.0.0.0**).
   - *Auto Negotiate*.
   - *Speed*.
   - *Duplex*.

   Only the *IP Address*, *Subnet Mask*, and *Gateway Address* fields are configurable.
10. Change the IP address, subnet mask, and gateway address as directed by the customer. To change the addresses, type the following at the **C >** prompt and press **Enter**.

ipconfig ***xxx.xxx.xxx.xxx yyy.yyy.yyy.yyy zzz.zzz.zzz.zzz***

The IP address is ***xxx.xxx.xxx.xxx***, the subnet mask is ***yyy.yyy.yyy.yyy***, and the gateway address is *zzz.zzz.zzz.zzz*, where the octets ***xxx***, ***yyy***, and *zzz* are decimals from zero through 255. If an address is to remain unchanged, type the current address in the respective field.

11. Select *Exit* from the *File* pull-down menu. A HyperTerminal message box appears.
12. Click *Yes*. A second message box appears.
13. Click *No* to exit and close the application.
14. Power off the maintenance terminal and disconnect the RS-232 modem cable. Replace the protective cap over the maintenance port.
15. Perform a POR (*IML or reset switch*).
16. Connect the product to the customer-supplied Ethernet LAN segment or Ethernet hub:
    a. Connect one end of the Ethernet patch cable (supplied) to the RJ-45 connector (labelled **10/100**).
    b. Connect the remaining end of the cable to the LAN as directed by the customer or to any available Ethernet hub port.
17. Go to *Task 6: Configure server password and network addresses*.

Task 6: Configure server password and network addresses

Ensure that the LAN is installed. If the server or equipment cabinet is installed on a dedicated LAN, network information does not require change. Change the default password for the server LCD panel (if required by the customer), then go to *Task 7: Configure management server information*.

If the server or equipment cabinet is installed on a public LAN, the default password for the server LCD panel and the following transmission control protocol internet protocol (TCP/IP) network information must be changed to conform to the customer's LAN addressing scheme:

- IP address.
- Subnet mask.

Configure password

To configure a new LCD panel password:

1. Press **ENTER** on the management server LCD panel. The **Welcome!!** or operational information message changes to an **Input Password 0****** message.
2. Using the ▲ button to increment a digit, the ▼ button to decrement a digit, the ◄ button to move the cursor left, and the ► button to move the cursor right, input the default password (**9999**), and press **ENTER**. A **LAN 1 Setting??** message appears at the LCD panel.
3. Press the ▼ button several times until the **Change Password?** option appears at the LCD panel, then press **ENTER**. A **New Password 0****** message appears.
4. Use the arrow keys as described in step 2 to input a new 4-digit numeric password, then press **ENTER**. A **Save Change? Yes, Save!!** message appears.
5. Press **ENTER**. A **Wait a moment!** message appears at the LCD panel, the LCD panel returns to the **LAN 1 Setting??** message, and the password changes.

Configure private LAN addresses

To configure TCP/IP network information for the private LAN connection (LAN 2) use the following steps:

1. Press **ENTER** on the management server LCD panel. The **Welcome!!** or operational information message changes to an **Input Password 0****** message.
2. Using the ▲ button to increment a digit, the ▼ button to decrement a digit, the ◄ button to move the cursor left, and the ► button to move the cursor right, input the default or changed password, and press **ENTER**. The **LAN 1 Setting??** message appears at the LCD panel.
3. Press the ▼ button. The **LAN 2 Setting??** message appears at the LCD panel. Press **ENTER** and the default IP address of **10.1.1.1** appears.
4. Use the arrow keys as described in step 2 to input a new IP address, then press **ENTER**. A **Save Change? Yes, Save!!** message appears.

5. Press **ENTER**. The LAN 2 IP address changes and the default subnet mask of **255.0.0.0** appears.
6. Use the arrow keys as described in step 2 to input a new subnet mask, then press **ENTER**. A **Save Change? Yes, Save!!** message appears.
7. Press **ENTER**. A **Wait a moment!** message appears at the LCD panel, the panel returns to the **LAN 1 Setting??** message, and the LAN 2 subnet mask changes.
8. Record the private LAN IP address and subnet mask for reference if the server hard drive fails and must be restored.

Configure public LAN addresses (optional)

To optionally configure TCP/IP network information for the public LAN connection (LAN 1), use the following steps:

1. Press **ENTER** on the management server LCD panel. The **Welcome!!** or operational information message changes to an **Input Password 0****** message.
2. Using the ▲ button to increment a digit, the ▼ button to decrement a digit, the ◄ button to move the cursor left, and the ► button to move the cursor right, input the default or changed password, and press **ENTER**. The **LAN 1 Setting??** message appears at the LCD panel.
3. Press **ENTER** and the default IP address of **192.168.0.1**. appears.
4. Use the arrow keys as described in step 2 to input a new IP address, then press **ENTER**. A **Save Change? Yes, Save!!** message appears.
5. Press **ENTER**. The LAN 1 IP address changes and the default subnet mask of **255.0.0.0** appears.
6. Use the arrow keys as described in step 2 to input a new subnet mask, then press **ENTER**. A **Save Change? Yes, Save!!** message appears.
7. Press **ENTER**. A **Wait a moment!** message appears at the LCD panel, the panel returns to the **LAN 1 Setting??** message, and the LAN 1 subnet mask changes.
8. Record the public LAN IP address and subnet mask for reference if the server hard drive fails and must be restored.

Task 7: Configure management server information

Follow the procedure in this section, to configure a server computer name and workgroup name from the Windows operating system, using a LAN-attached PC with standard web browser.

If required, change the server's gateway addresses and domain name system (DNS) server IP addresses to conform to the customer's LAN addressing scheme. The gateway addresses are the addresses of the local router for the corporate intranet.

Access the management server desktop

To login and access the server desktop, use the following steps:

1. Ensure that the management server and a browser-capable PC are connected through an Ethernet LAN. At the PC, launch the browser application (Netscape Navigator or Internet Explorer).
2. Enter the **LAN 2** IP address of the server, followed by **:5800**, as the Internet uniform resource locator (URL). Use the following format:

   http://xxx.xxx.xxx.xxx:5800

   Where ***xxx.xxx.xxx.xxx*** is the default IP address of **10.1.1.1** or the IP address configured while performing *Task 6: Configure server password and network addresses*. The *VNC Authentication* screen appears.
3. Type the default password and click *OK*. The *Welcome to Windows* dialog box appears.

   NOTE: The default TightVNC viewer password is **password.**

4. Click the **Send Ctrl-Alt-Del** button at the top of the window to log on to the server desktop. The *Log On to Windows* dialog box appears.

   NOTE: Do not simultaneously press the **Ctrl**, **Alt**, and **Delete** keys. This action logs the user on to the browser-capable PC, not the server.

5. Type the default Windows user name and password and click *OK*. The server's Windows desktop opens and the *EFCM Log In* dialog box appears.

NOTE: The default Windows user name is **Administrator** and the default password is **password**. Both are case-sensitive.

Configure management server names

To configure the management server name and workgroup name, use the following steps:

1. Open the *System* window on your Windows desktop (*Start>Settings>Control Panel>System*). The *System Properties* dialog box appears with the *General* tab open by default.
2. Click the *Network Identification* tab. The *System Properties* dialog box appears with the *Network Identification* tab selected.
3. Click *Properties*. The *Identification Changes* dialog box appears (Figure 23).

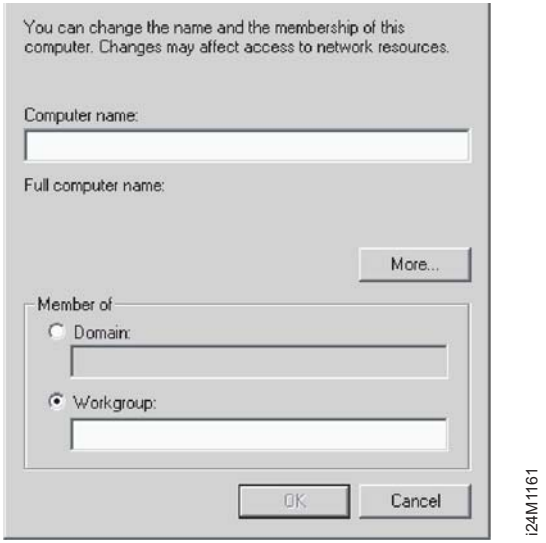


Figure 23 Identification Changes Dialog Box

4. Change the name to **MGMTSERVER** in the *Computer Name* field. Click (select) the *Workgroup* radio button, change the name to **WORKGROUP**, and click *OK*. The dialog box closes.
5. Record the computer and workgroup names for reference if the server hard drive fails and must be restored.
6. Close all dialog boxes and return to the Windows desktop.

Configure gateway and DNS server addresses

To configure gateway and DNS server IP addresses for the private LAN connection (**LAN 2**) and public LAN connection (**LAN 1**) use the following steps:

1. At the Windows desktop, click *Start* at the left side of the task bar (bottom of the desktop), then sequentially select *Settings*, *Control Panel*, and *Network and Dial-up Connections*. The *Network and Dial-up Connections* window appears.
2. Double-click the *Local Area Connection 2* icon to configure addresses for the private LAN connection (**LAN 2**). The *Local Area Connection 2 Status* dialog box appears.
3. Click *Properties*. The *Local Area Connection 2 Properties* dialog box appears.
4. Double-click the *Internet Protocol (TCP/IP)* entry in the *Components checked are used by this connection* field. The *Internet Protocol (TCP/IP) Properties* dialog box appears (Figure 24).

   The *Use the following IP address* radio button is enabled and the *IP address* and *Subnet mask* fields display network information configured while performing *Task 6: Configure server password and network addresses*.
5. Enter the gateway address obtained from the customer in the *Default gateway* field.
6. Select (enable) the *Use the following DNS server addresses* radio button. At the *Preferred DNS server* field, enter the DNS server IP address obtained from the customer, then click *OK* to apply the changes and close the dialog box.

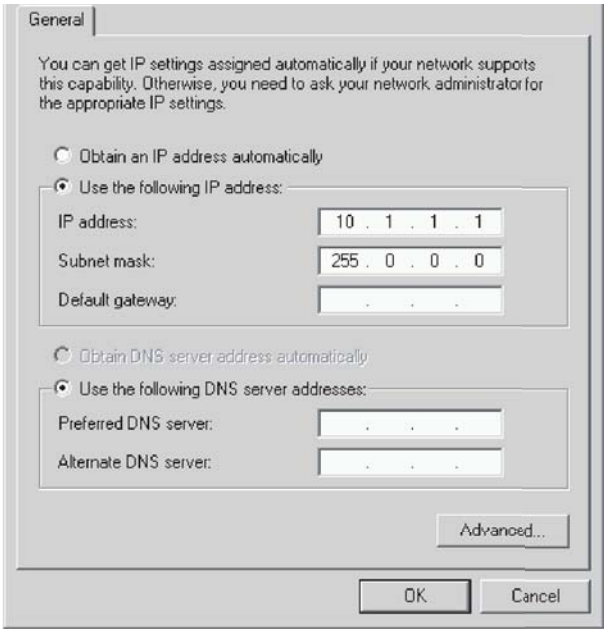

General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
10 . 1 . 1 . 1
Subnet mask:
255 . 0 . 0 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel
I24M1163

Figure 24 Internet Protocol (TCP/IP) Properties dialog box

7. Close dialog boxes as appropriate and return to the The *Network and Dial-up Connections* window.
8. Record the changed gateway and DNS server addresses for reference if the server hard drive fails and must be restored.
9. Double-click the *Local Area Connection 1* icon to optionally configure addresses for the public LAN connection (**LAN 1**), and repeat step 2 through step 8.
10. Close all dialog boxes and return to the Windows desktop.
11. Reboot the server and *Access the management server desktop*.

Task 8: Configure Windows operating system users

Follow the procedures in this section to configure password access for all authorized Windows (server) users. It is also recommended to change the default administrator password.

To configure users use the following steps:

1. At the Windows desktop, click *Start* at the left side of the task bar (bottom of the desktop), then sequentially select *Settings*, *Control Panel*, and *Users and Passwords*. The *Users and Passwords* dialog box appears.
2. The *Guest* user name is a built-in account in the Windows operating system and cannot be deleted. The *srvacc* account is for field service users and must not be modified or deleted.

Change default administrator password

To change the administrator password from the default (**password**) to a customer-specified password use the following steps:

1. Click *Set Password* on the *Users and Passwords* dialog box. The *Set Password* dialog box appears.
2. Type the new password in the *New Password* and *Confirm New Password* fields. Both fields are case-sensitive.
3. Click *OK*. The default administrator password changes and the *Set Password* dialog box closes.

Add a new user

To set up a new Windows user use the following steps:

1. Click *Add* on the *Users and Passwords* dialog box. The first window of the *Add New User* wizard appears (Figure 25).
2. Type the appropriate information in the *User name* and *Domain* fields and click *Next*. The second window of the *Add New User* wizard appears.
3. Type the new user password in the *Password* and *Confirm password* fields and click *Next*. The third window of the *Add New User* wizard appears.
4. Select the *Standard user*, *Restricted user*, or *Other* radio button based on the access level granted for each user. If the *Other* radio button is selected, choose the type of access from the adjacent list box.

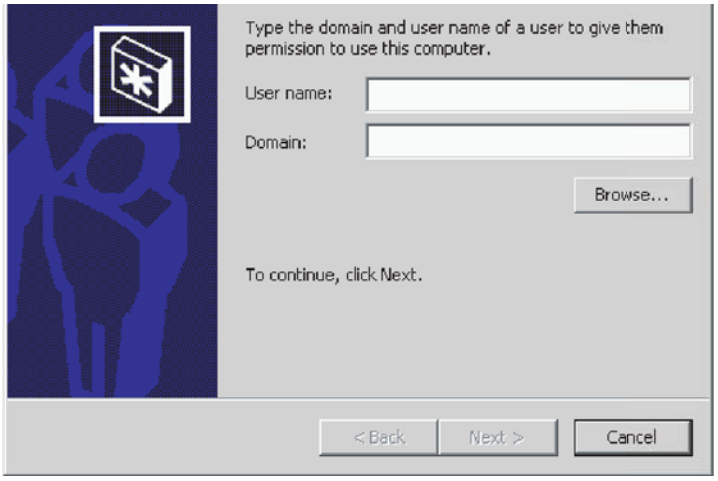


Figure 25 Add New User wizard

5. Click *Finish*. New user information is added and the wizard closes. Record the user information for reference if the server hard drive fails and must be restored.
6. If no other users are to be added, close all dialog boxes and return to the Windows desktop.

Change user properties

To change existing user properties use the following steps:

1. At the *Users and Passwords* dialog box, highlight the user at the *Users for this computer* field and click *Properties*. The *Properties* dialog box appears with the *General* tab selected (Figure 26).
2. Type the appropriate new user information in the *User name*, *Full name*, and *Description* fields, then click the *Group Membership* tab. The *Properties* dialog box appears with the *Group Membership* tab selected.
3. Select the *Standard user*, *Restricted user*, or *Other* radio button based on the level of access to be changed. If the *Other* radio button is selected, choose the type of access from the adjacent list box.

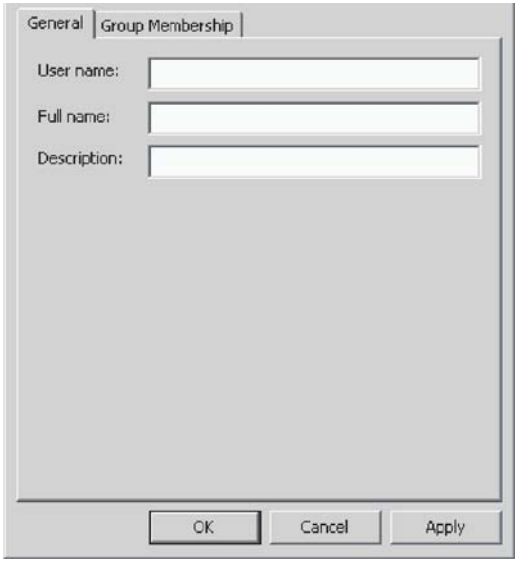


Figure 26 Properties dialog box (General tab)

4. Click *OK*. The new user information is added and the *Properties* dialog box closes. Record the user information for reference if the server hard drive fails and must be restored.
5. If no other users are to be changed, close all dialog boxes and return to the Windows desktop.

Task 9: Set management server date and time

SAN Management application logs are stamped with the server date and time, and the product system clock is synchronized with the server date and time by default.

To set the server date and time, use the following steps:

1. At the Windows desktop, click *Start* at the left side of the task bar (bottom of the desktop), then sequentially select *Settings*, *Control Panel*, and *Date/Time*. The *Date/Time Properties* dialog box appears with the *Date & Time* page open.

NOTE: The *Time Zone* field must be set before the *Date & Time* field.

2. Click the *Time Zone* tab. The *Date/Time Properties* dialog box appears with the *Time Zone* page open (Figure 27).

Figure 27 Date/Time Properties dialog box (Time Zone tab)

3. To change the time zone:
   a. Select the appropriate time zone from the drop-down list at the top of the dialog box.
   b. Select the *Automatically adjust clock for daylight saving changes* check box, only if instructed by the customer.
   c. Click *Apply*. Record time zone and daylight savings information for reference if the server hard drive fails and must be restored.
4. Click the *Date & Time* tab. The *Date/Time Properties* dialog box appears with the *Date & Time* page open (Figure 28).
5. To change the date and time:
   a. Select the month from the drop-down list under *Date*.
   b. Click the up or down arrow adjacent to the year field and select the desired year.
   c. Click the day on the calendar to select the desired date.

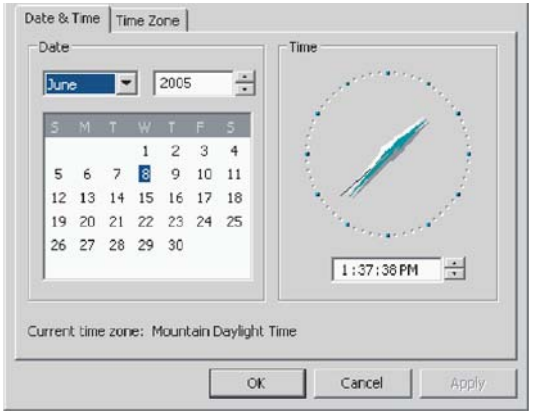


Figure 28 **Date/Time Properties dialog box (Date & Time tab)**

d. Click in the time field and enter the desired time; then click the adjacent up or down arrow and select *AM* or *PM*.

e. Click *Apply*. Record date and time information for reference if the server hard drive fails and must be restored.

6. Close all dialog boxes and return to the Windows desktop.

Task 10: Configure the call-home feature (optional)

The management server has an optional call-home feature that provides automatic dial-out through the internal modem to a service support facility to report switch problems. The problem is logged into the support facility's tracking system for resolution.

To configure the call-home feature, use the following steps:

1. Ensure that a telephone cable is routed and connected to the **LINE** jack at the rear of the management server (connected while performing *Task 6: Configure server password and network addresses*). There are two jacks on the server internal modem; one for the call-home connection (**LINE**), and the other for a telephone (**PHONE**).

2. Double-click the *Call Home Configuration* icon on your Windows desktop. The *Call Home Configuration* dialog box appears.

3. Type the telephone number of IBM support in the *Call Center Phone Number* field. Include necessary information, such as the country code, area code, or any prefix required to access a telephone line outside the facility.
4. Type the telephone number for access to the local server in the *Local Phone Number* field. Include necessary information such as the country code or area code.
5. Click *OK* to save the configured telephone numbers and close the dialog box.

Task 11: Assign user names and passwords

In addition to password access for the Windows operating system, users must be configured for SAN management application access.

To assign user names and passwords for the SAN management application (EFCM), use the following steps:

1. Open the EFCM application. The EFCM log in dialog box appears.
2. Type the SAN management application default user ID and password and select a server or IP address from the *Network Address* drop-down list.

   NOTE: The default user ID is **Administrator** and the default password is **password.** Both are case-sensitive.

3. Click *Login*. The application opens and the EFCM main window appears.
4. Select *Users* from the *SAN* menu (*SAN>Users*). The *EFCM Server Users* dialog box appears.
5. Click *Add*. The *Add User* dialog box appears (Figure 29).

Figure 29 Add User dialog box

6. Enter information in fields as directed by the customer:
   - **Description -** Type a new user name (less than 16 alphanumeric characters). Control characters and spaces are not valid. The user name is case-sensitive.
   - **Email Address -** Type one or more new user e-mail addresses. Separate multiple addresses with a semicolon.
   - **User ID -** Type a unique user ID for the new user.
   - **Secure password -** Type a password (less than 16 alphanumeric characters). Control characters and spaces are not valid. The password is case-sensitive.
   - **Retype Password -** To confirm the password, enter the password exactly as in the *Secure Password* field.
7. Enable (check) the *Enable* check box to enable e-mail notification for the new user.
8. Select (click) the *Filter* link to configure event types for which e-mail notification is sent. The *Define Filter* dialog box appears. For instructions on defining event filters, refer to the *EFC Manager Software Release 8.7 User Manual* (620-000170).
9. Click *OK* to accept the information. Close all dialog boxes and return to the EFCM main window.

Task 12: Configure the product to the management application

The SAN management application should be able to discover and identify a new switch before starting to manage it.

For the SAN management application to identify the switch, use the following steps:

1. Select *Setup* from the *Discover* menu (*Discover>Setup*) in the EFCM main window. The *Discover Setup* dialog box appears.
2. Click *Add*. The *Address Properties* dialog box appears with the *IP Address* page open by default (Figure 30).

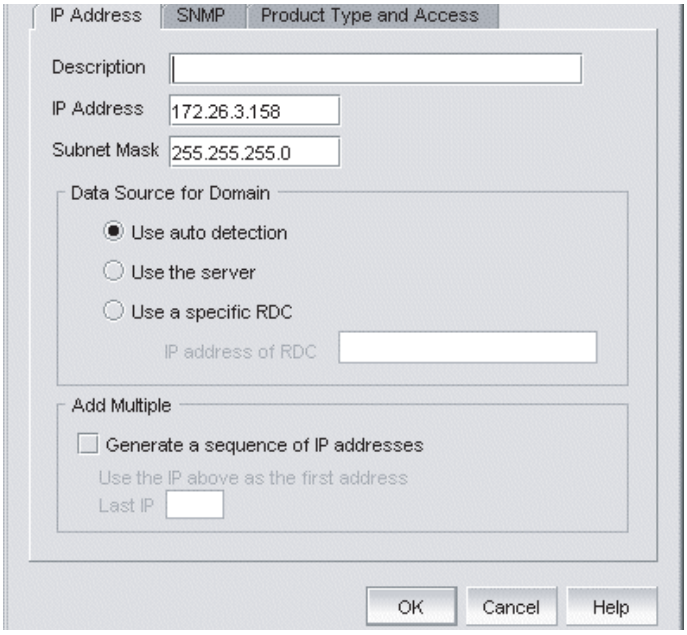


Figure 30 Address Properties dialog box (IP Address page)

3. Type a description for the product in the *Description* field.
4. Type the product IP address (determined by the customer) in the *IP Address* field.
5. Type the product subnet mask (determined by the customer) in the *Subnet Mask* field.

6. Click *OK* to save the entered information and define the switch to the SAN management application. Close all dialog boxes and return to the EFCM main window.

Task 13: Record or verify server restore information

The Windows operating system configuration information must be recorded to restore the server in case of hard drive failure.

Record or ensure the following information:

1. Network configuration information was recorded while performing *Task 6: Configure server password and network addresses* and *Task 7: Configure management server information*.
   a. Default LCD panel password (**9999**) or changed password was recorded.
   b. Default or changed network addresses were recorded for the private LAN connection **(LAN 2**):
      - **IP address -** default is **10.1.1.1**.
      - **Subnet mask -** default is **255.0.0.0**.
      - **Gateway address -** default is blank.
      - **DNS server IP address -** default is blank.
   c. Default or changed network addresses were recorded for the public LAN connection (**LAN 1**):
      - **IP address -** default is **192.168.0.1**.
      - **Subnet mask -** default is **255.0.0.0**.
      - **Gateway address -** default is blank.
      - **DNS server IP address -** default is blank.
   d. Default computer name (**MGMTSERVER**) or changed computer name was recorded.
2. User passwords and other information were recorded while performing *Task 8: Configure Windows operating system users*.
3. Date and time information was recorded while performing *Task 9: Set management server date and time*.

a. Time zone was recorded.

b. Management server was set to automatically adjust the clock for daylight savings time changes.

4. Record the product's ID number:

   a. Open the *System Properties* dialog box by double-clicking the *System* icon in the Windows control panel (*Start>Settings>Control Panel*). The *System Properties* dialog box appears with the *General* tab open by default.

   b. Note down the product's ID number listed under the *Registered to* heading.

   c. Close all dialog boxes and return to the Windows desktop.

Task 14: Verify product-to-server communication

Communication must be verified between the product and server (SAN management and Element Manager applications).

To ensure that a communication has been established between the product and the server, use the following steps:

1. Inspect the shape and color of the status symbol associated with the product icon in the SAN management application main window (physical map or product list). Table 4 explains operational states and associated symbols.

Table 4 Operational states and symbols

Operational state	Status symbol
Operational - Communication is established, the product is operational, and no failures are indicated. Go to *Task 15: Configure PFE key (optional)*.	No status symbol
Degraded - Communication is established, but the product is operating in degraded mode and requires service. This condition is typical if a port or redundant CRU fails. Go to step 2.	
Failed - Communication is established, but the product failed and requires immediate service. Go to step 2.	
Status Unknown - Product status is unknown because of a network communication failure. Go to step 2.	

2. Right-click the product icon at the SAN management application's physical map. A pop-up menu appears.
3. Select the *Element Manager* option from the pop-up menu. When the Element Manager application opens, the last view accessed by a user opens by default. As an example, the *Hardware* view (Figure 31) is shown.

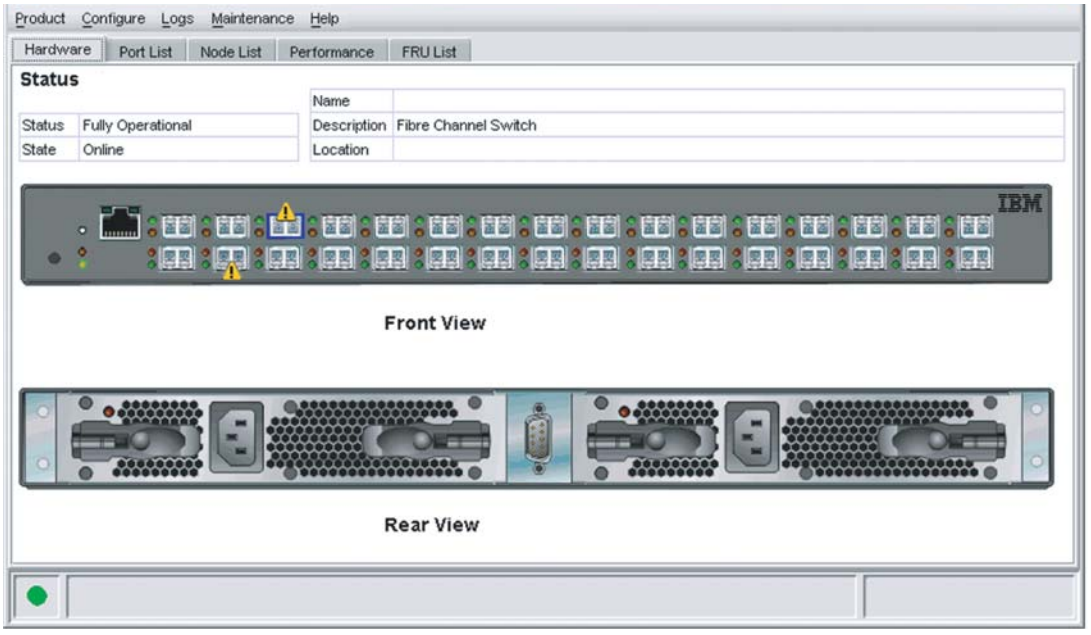


Figure 31 Hardware View

4. Inspect product status at the *Hardware* view and perform one of the following steps:
   - If the product appears operational (no CRU alert symbols and a green circle at the status bar), go to *Task 15: Configure PFE key (optional)*.
   - If product operation appears degraded or a failure is indicated (CRU alert symbols and a yellow triangle or red diamond on the status bar), go to *MAP 0000: Start MAP* to isolate the problem.

Task 15: Configure PFE key (optional)

Follow the procedures in this section to install optional features using PFE key.

After purchasing a feature, obtain the PFE key by following the enclosed instructions. The key is an alphanumeric string consisting of uppercase and lowercase characters that must be entered exactly, including dashes. An example format is:

XxXx-XXxX-xxXX-xX.

NOTE: PFE keys are encoded to work with the serial number of the installed switch only. Record the key to re-install the feature if required. If the switch fails and must be replaced, obtain new PFE keys from IBM. Please have the serial numbers of the failed and replacement switches, and the old PFE key number or transaction code.

The optional features that you can install using PFE keys are listed below:

- **Element Manager application -** This feature enables out-of-band product management through an Element Manager interface. Products are delivered with the application enabled for a 31-day grace period. Before grace period expiration, the application must be reactivated through a PFE key.

  During the grace period, a *No Feature Key* dialog box appears when the Element Manager application opens. Click *OK* to close the dialog box and use the application. In addition, the message **Element Manager license key has not been installed - Please follow up instructions to update permanent key** appears splashed across all views.

- **FICON management server -** These feature supports inband product management through FMS host control.

- **Flexport Technology** - A Flexport Technology product is delivered at a discount with all Fibre Channel ports disabled. When additional port capacity is required, the remaining ports are incrementally enabled through this feature.

- **Full volatility -** This feature ensures no Fibre Channel frames are stored after the product is powered off or fails, and a memory dump file (that possibly includes classified data frames) is not included as part of the data collection procedure.

- **N_Port ID virtualization -** This feature allows up to 256 Fibre Channel addresses to be assigned to an N_Port.
- **SANtegrity binding -** This feature enhances security in SANs with a large and mixed group of fabrics and attached devices.
- **SANtegrity authentication -** This feature enhances security of the product by controlling the ability of users, devices, and processes to attach to the product.
- **OpenTrunking -** This feature provides dynamic load balancing of Fibre Channel traffic across multiple ISLs.

To install the optional features using Element Manager of the switch, use the following steps:

1. Select *Features* from the *Configure* menu (*Configure>Features*). The *Configure Feature Key* dialog box appears.
2. Click *New*. The *New Feature Key* dialog box appears (Figure 32).

Figure 32 New Feature Key dialog box

3. Type the PFE key (case-sensitive **xxxx-xxxx-xxxx-xx** format) and click *OK*. The *Enable Feature Key* dialog box appears.
4. Ensure that the feature description appears in the *New Features* panel and click *OK*. A *Warning* dialog box appears with the message **Installing this feature key causes an IPL and momentary loss of the LAN connection. The operation is nondisruptive to Fibre Channel traffic. Do you wish to continue?**
5. Click *Yes* to enable the PFE key and IPL the product. Close all dialog boxes and return to the Element Manager application.

Task 16: Configure management server (optional)

Follow the procedures in this section to configure the open systems management server (OSMS) and enable OSI host control of the product.

- **Open systems management server -** Implementing and enabling OSI host control of the product requires installation of a SAN management application on the OSI server. Applications include Veritas SANPoint Control or Tivoli NetView.
- **FICON management server -** Implementing and enabling FICON host control of the product requires installation of the IBM System Automation for OS/390™ (SA OS/390™) or z/OS® operating system. In addition, the FICON management server PFE key must be installed. Refer to *Task 15: Configure PFE key (optional)* for instructions.

OSMS

To configure the open systems management server use the following steps:

1. Select *Open Systems Management Server* from the *Configure* menu (*Configure>OSMS*). Two submenu options appears:
   - *Enable OSMS*.
   - *Host Control Prohibited*.
2. Select (check) *Enable OSMS* to enable OSMS. Check the box to enable the server.
3. Select (check) *Host Control prohibited* to prohibit a host management program from changing configuration and connectivity parameters on the product. The host program has read-only access to configuration and connectivity parameters.

FMS

To configure the FICON management server using Element Manager, use the following steps:

FICON Only

1. Select *FICON Management Server* from the *Configure* menu (*Configure>FICON Management Server*). Three submenu options appear:
   - *Enable FMS*.
   - *Parameters*.
   - *Zoning*.
2. Enable or disable FMS by selecting the *Enable FMS* option. Check the box to enable the server.
3. Click *Parameters*. The *Configure FICON Management Server* dialog box appears (Figure 33).

Figure 33 Configure FICON Management Server dialog box

   a. Select (check) the *Switch Clock Alert Mode* field, to enable the parameter. When enabled, a warning message appears, if the product is set to periodically synchronize date and time with the management server. This process may conflict with the date and time set from the attached FICON host.

   b. Select (check) the *Host Control Prohibited* field to enable the parameter. When enabled, this option prohibits FICON host control of the product.

c. Select (check) the *Programmed offline state control* field, to enable the parameter. When enabled, this option allows an attached FICON host to set the product online or offline.

d. Select from the *Missing Interrupt Handler Timeout (MIHPTO)* drop-down list to select a value. Available selections range from 15 seconds to 10 minutes. The MIHPTO value is the response time a host allows from a product before timing out the FICON link. Large fabrics require a large value.

e. Click *Activate* to enable changes and close the dialog box.

4. Click *Zoning*. The *Configure FICON Management Server Zoning* dialog box appears (Figure 34).

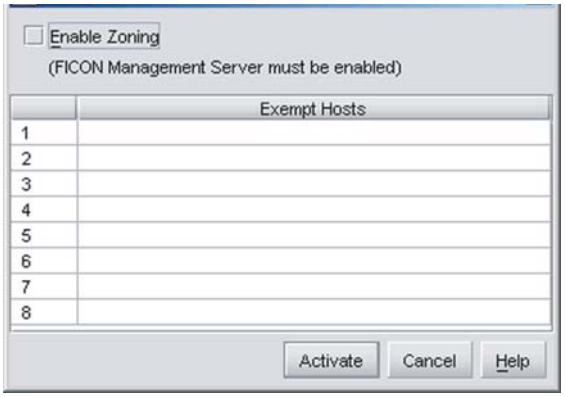


Figure 34 Configure FICON Management Server Zoning dialog box

a. Select (check) *Enable Zoning* to enable FICON control unit port (CUP) zoning.

b. Type the WWN of servers to be configured as partitioned hosts. Partitioned host queries regarding status of zoned devices are filtered by zoning data.

c. Click *Activate* to enable changes and close the dialog box.

Task 17: Set product date and time

Log entries are stamped with the date and time received from the product.

To set the date and time for the product using the Element Manager, use the following steps:

1. Select *Operating Parameters* from the *Configure* menu (*Configure>Operating Parameters*). The *Operating Parameters* view appears.
2. Click the *Date/Time* tab (Figure 35).

   Date and time can be set manually, or set to be periodically updated by the SAN management application (the product and application synchronize at least once daily).

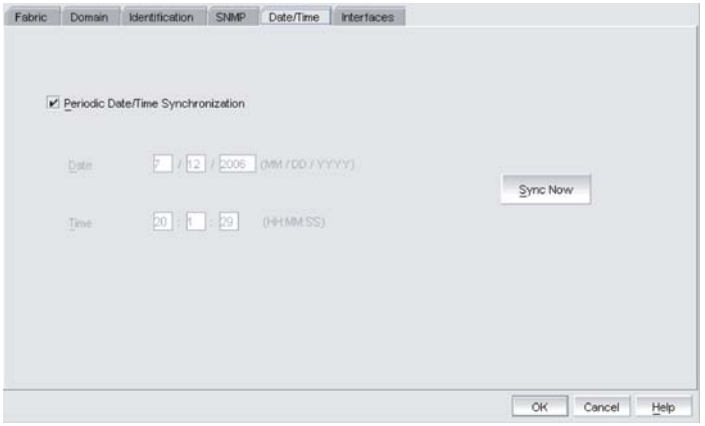


Figure 35 Configure Date and Time dialog box

3. Use the following procedure to set the date and time manually:
   a. Disable (uncheck) the *Periodic Date/Time Synchronization* check box. The *Date* and *Time* fields become active.
   b. Change the date using the following format.
      - Month (*MM*): **1 - 12**.
      - Day (*DD*): **1 - 31**.
      - Year (*YYYY*): greater than **1980**.
   c. Change the time using the following format:
      - Hour (*HH*): **0 - 23**.
      - Minute (*MM*): **0 - 59**.
      - Second (*SS*): **0- 59**.

d. Click *Activate* to set the switch date and time and close the dialog box.

4. Use the following procedure to set the product to periodically synchronize date and time with the SAN management application:

   a. Enable (check) the *Periodic Date/Time Synchronization* check box.

   b. Do one of the following:

      - Click *OK* to enable synchronization and close the dialog box.

        Switch date and time synchronize with the SAN management application date and time at the next update period (at least once daily)

        or

      - Click *Sync Now* to synchronize the switch and SAN management application immediately.

      - The *Date and Time Synced* information dialog box appears. Click *OK* to synchronize the date and time and close the dialog box; then click *OK* to enable synchronization. Close the *Configure Date and Time* dialog box.

Task 18: Configure the Element Manager application

To configure the Element Manager application, selectively perform the following tasks according to customer requirements:

Product	• Identification • Product parameters • Fabric parameters.
Ports	• Basic information • Buffer-to-buffer credits (BB_Credits) • N_Port identifier virtualization (NPIV).

Management	• SNMP trap message recipients • Threshold alerts • EFCM Basic Edition interface access • Telnet access • e-mail, Ethernet event, and call-home event notification.
Security	• SANtegrity authentication • Enterprise Fabric Mode • SANtegrity binding.
Interswitch links	• OpenTrunking • Preferred path • ISL port fencing

Configure product identification

Follow the procedures in this section to configure the product's identification using the Element Manager.

NOTE: The *Name*, *Location*, and *Contact* variables correspond respectively to the SNMP variables *sysName*, *sysLocation*, and *sysContact*, and are used by management workstations when obtaining product data.

1. Select *Operating Parameters* from the *Configure* menu (*Configure>Operating Parameters*). The *Operating Parameters* dialog box appears.
2. Click the *Identification* tab (Figure 36).

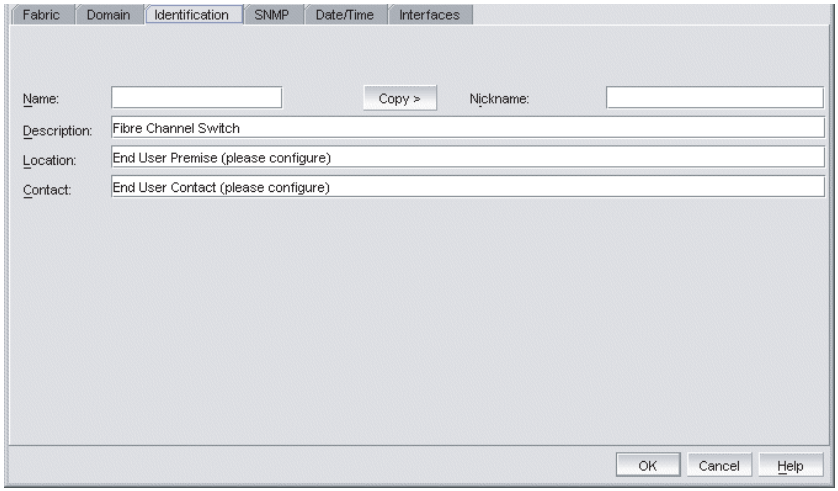


Figure 36 Configure Identification dialog box

a. Type a unique product name (less than 24 alphanumeric characters) in the *Name* field. If the product is installed on a public LAN, the name should reflect the network DNS host name.

b. Type a product nickname name (less than 24 alphanumeric characters) in the *Nickname* field. The nickname appears instead of the WWN in Element Manager application views.

c. Type a description (less than 255 alphanumeric characters) in the *Description* field.

d. Type the physical location (less than 255 alphanumeric characters) in the *Location* field.

e. Type the name of a contact person (less than 255 alphanumeric characters) in the *Contact* field.

3. Click *Activate* to save the information and close the dialog box.

Configure product parameters

Follow the procedures in this section to configure the domain parameters of the product using the Element Manager.

To configure the domain parameters for the product, use the following steps:

1. Set the product offline. Refer to *Set online state* for instructions.
2. Select *Operating Parameters* from the *Configure* menu (*Configure>Operating Parameters*).
3. Click the *Domain* tab (Figure 37).

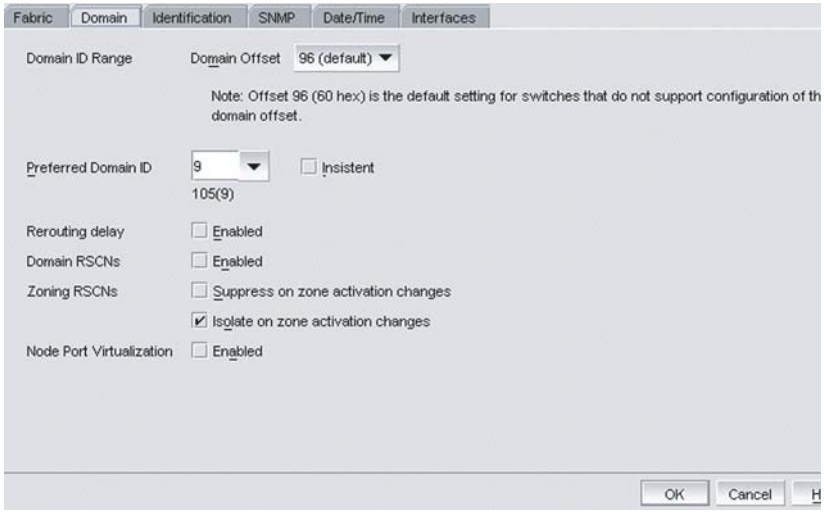


Figure 37 Configure Switch Parameters dialog box

a. Select the *Domain ID Offset* value from the drop-down list. Values available in the drop-down list are 0, 32, 64, 96 (default), 128, 160, and 192. Domain IDs minus the offset are still in the 1-31 range.

b. Type a value between **1 - 31**in the *Preferred Domain ID* field. This value uniquely identifies each fabric element.

NOTE: An ISL between fabric elements with identical domain IDs segments and prevents communication.

If the *Insistent Domain ID* field is enabled (checked), the value configured in the *Preferred Domain ID* field becomes the active domain ID when the fabric initializes.

c. Enable (check) the *Rerouting Delay* field if you want the traffic to be delayed through the fabric by the user-specified error detect time out value (E_D_TOV). This delay ensures that Fibre Channel frames are delivered to their destination in order.

d. Enable (check) the *Domain RSCNs* field if you want the attached devices to register to receive notification when other devices change state.

e. Enable (check) the *Suppress Zoning RSCNs on Zone Set Activations* field if you do not want the RSCNs to be transmitted when a zone set is activated.

f. Enable (check) the *Isolate on zone activations* field if you want only devices that require RSCN notification, due to a zoning configuration change, to receive RSCNs. Do not enable this option if *Suppress on zone set activations* is enabled because RSCNs will not be sent to attached devices.

g. Enable (check) the *Node Port Virtualization* field for N_Port identifier virtualization (NPIV). NPIV allows multiple (up to 256) Fibre Channel addresses to be assigned to a node (N_Port).

4. Click *OK* to save the information and close the dialog box.
5. Set the product online. Refer to *Set online state* for instructions.

Configure fabric parameters

Follow the procedures in this section to configure fabric operating parameters.

To configure the fabric operating parameters, use the following steps:

1. Set the product offline. Refer to *Set online state* for instructions.
2. Select *Operating Parameters* from the *Configure* menu (*Configure*>*Operating Parameters*). The *Operating Parameters* dialog box appears.
3. Click the *Fabric* tab(Figure 38).

Figure 38 Configure Fabric Parameters dialog box

a. Type a value between **10** - **1200** tenths of a second (1-120 seconds) in the *R_A_TOV* field. This value must be greater than the E_D_TOV value.

b. Type a value between **2** - **600** tenths of a second (0.2 - 60 seconds) in the *E_D_TOV* field. This must be greater lesser than the R_A_TOV value.

NOTE: Fabric elements must be set to the same R_A_TOV and E_D_TOV values. An ISL between fabric elements with different values segments and prevents communication.

---

c. Select from the *Switch Priority* drop-down list to assign a priority for the switch. The available options are *Default*, *Principal*, and *Never Principal*.

The principal switch is assigned a priority of **1** and controls the allocation and distribution of domain IDs for all fabric elements (including itself).

NOTE: At least one switch in a fabric must be set as *Principal* or *Default*. If all switches are set to *Never Principal*, all ISLs segment.

---

d. Select one of the options in the *Interop Mode* drop-down list to set the switch operating mode. This setting only affects the mode used to manage the switch; it does not affect port operation.

The available options are:

- **McDATA Fabric 1.0 -** Select this option if the product is fabric-attached only to other McDATA directors or switches operating in McDATA fabric mode.
- **Open Fabric 1.0 -** Select this option (default) for managing heterogeneous fabrics and if the product is fabric-attached to McDATA directors or switches and open-fabric compliant switches produced by other OEMs.

e. Select from one of the options to change the ISL cost.

- **By Port Speed:** Select if you want FSFP routing selection to account for port speed when assigning traffic to ISLs.
- **Ignore Port Speed**: Select if you do not want FSFP routing selection to account for port speed when assigning traffic to ISLs. All ISLs have equal cost.

4. Click *OK* to save the information and close the dialog box.
5. Set the product online. Refer to *Set online state* for instructions.

Configure ports

Follow the procedure in this section to configure the ports for the product.

To configure Fibre Channel ports, use the following steps:

1. Select *Ports* from the *Configure* menu (*Configure>Ports*). The *Configure Ports* dialog box appears (Figure 39).

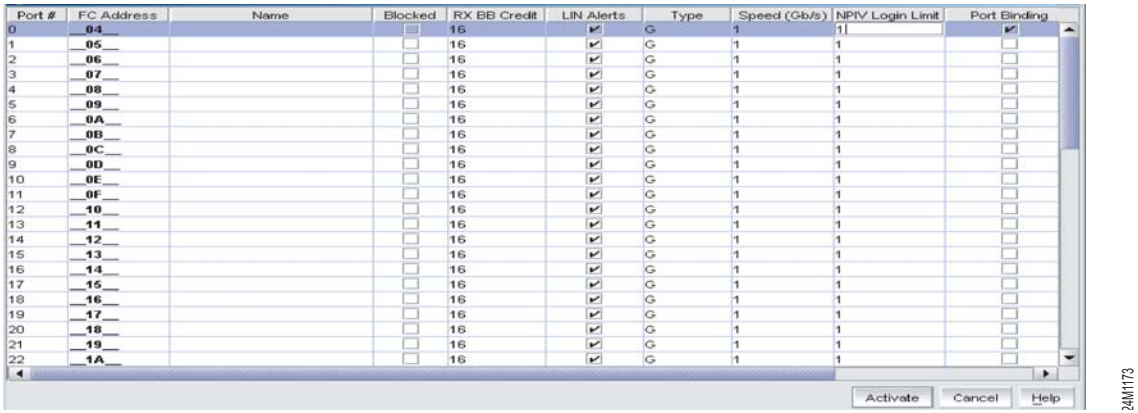


Figure 39 Configure Ports dialog box

a. Type a port name (less than 24 alphanumeric characters) in the *Name* field. The port name should characterize the device to which the port is attached.

b. Enable/Disable (Check/Uncheck) the *Blocked* check box to block or unblock the switch.

c. Type the desired value for buffer credits in the *RX BB Credit* column.

   The switch provides two port buffer pools of 235 receive BB_Credits each (470 credits total). Ports **0** through **3**, **8** through **11**, **16** through **19**, and **24** through **27** share buffer pool zero. Ports **4** through **7**, **12** through **15**, **20** through **23**, and **28** through **31** share buffer pool one. Each port can be assigned between two and 120 credits, provided the total credits allocated to all ports in a pool does not exceed 235. The default value is 12 credits per port.

d. Enable (check) the check box in the *LIN Alerts* column to enable link incident (LIN) alerts (default is enabled).

   When the feature is enabled and an incident occurs on the port link, an alert indicator (yellow triangle) is displayed at the *Hardware* view, and a message is sent to configured e-mail recipients.

e. Enable (check) the check box in the *FAN* column to enable the fabric address notification feature (default is enabled).

   When the feature is enabled, an FL_Port transmits FAN frames after loop initialization to ensure that FC-AL devices are still logged in.

f. Select the port type (E, F, or G) in the *Type* column to configure the port as E_Port, F_Port or G_Port.

g. Select from the drop-down list in the *Speed* column to configure the port transmission rate. Available selections are auto-negotiate between speeds (**Negotiate**), 1.0625 Gbps operation (**1 Gb/sec**), 2.1250 Gbps operation (**2 Gb/sec**), and 4.2500 Gbps operation (**4 Gb/sec**).

h. Type a desired value (**1 - 256**) in the *NPIV Login Limit* column.The NPIV feature must be installed to allow multiple Fibre Channel addresses to be assigned to an N_Port (*Install PFE keys (optional)*).

i. Enable (check) *Port Binding* if you want the port to connect only to a device with a WWN listed in the *Bound WWN* column.

j. Type the WWN or nickname of the device attached to the port in the *Bound WWN* column.

   - If port binding is enabled and a WWN or nickname is displayed in the *Bound WWN* column, only the specified device can connect.
   - If port binding is enabled but no WWN or nickname is displayed in the *Bound WWN* column, no device can connect.
   - If port binding is disabled, any device can connect.

k. Click *Activate* to save the information and close the dialog box.

Configure SNMP

Follow the procedures in this section to configure names, write authorizations, addresses, and UDP port numbers for SNMP trap message recipients.

To configure SNMP for the recipient workstations, use the following steps:

1. Select *Operating Parameters* from the *Configure* menu. The *Operating Parameters* dialog box appears.
2. Select the *SNMP* tab (Figure 40).

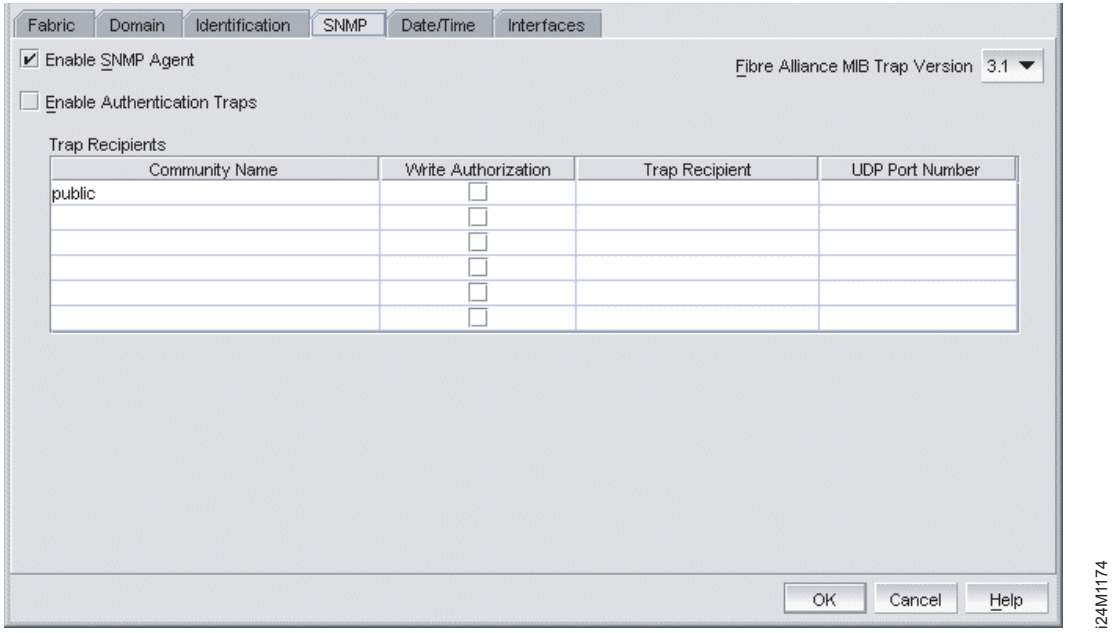


Figure 40 Configure SNMP dialog box

a. Click *Enable SNMP Agent* and *Enable Authentication Traps* to activate the installed agent and enable transmission of SNMP trap messages to recipients.

b. Select the appropriate FA MIB from the *Fibre Alliance MIB Trap Version* drop-down list. Valid selections are **FA MIB Version 3.0** or **FA MIB Version 3.1**.

c. Type a community name of less than 32 alphanumeric characters, for each configured recipient, in the *Community Name* field. This name is incorporated in SNMP trap messages to ensure against unauthorized viewing.

d. Enable (check) the *Write Authorization* column to enable write authorization for the trap recipient (default is disabled). When enabled, a configured user can change *sysContact*, *sysName*, and *sysLocation* SNMP variables.

e. Type the IP address or DNS host name of the trap recipient (SNMP management workstation) in the *Trap Recipient* field. It is recommended that the IP address be used.

f. Type a decimal port number in the *UDP Port Number* field to specify the UDP port number.

3. Click *Activate* to save the information and close the dialog box.

Configure threshold alerts

Follow the procedures in this section to set the threshold alerts for the product using the Element Manager.

A threshold alert notifies users when E_Port or F_Port transmit (Tx) or receive (Rx) throughput reaches or exceeds a specified value. Alerts are indicated by:

- An attention indicator (yellow triangle) associated with a port at the *Hardware* view, *Port List* view, or *Port Properties* dialog box.
- Data recorded in the *Threshold Alert Log*.

To configure threshold alerts use the following steps:

1. Select *Threshold Alerts* from the *Configure* menu (*Configure>Threshold Alerts*). The *Configure Threshold Alerts* dialog box appears. If alerts are configured, they display in table format showing the alert name, type, and state.
2. Click *New.* The *New Threshold Alert* dialog box appears (Figure 41).

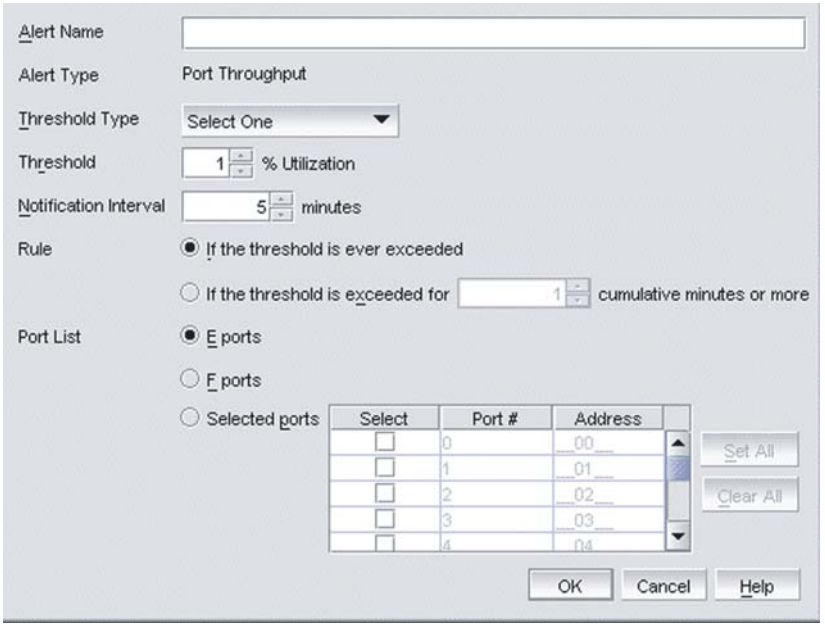


Figure 41 New Threshold Alert dialog box

3. Type a name (less than 64 alphanumeric characters) in the *Alert Name* field.
4. Select from the *Threshold Type* drop-down list to configure the alert type. Available selections are:
   - **Receive -** An alert occurs if the threshold value for receive throughput is reached or exceeded.
   - **Transmit -** An alert occurs if the threshold value for transmit throughput is reached or exceeded.
   - **Receive and Transmit -** An alert occurs if the threshold value for either throughput is reached or exceeded.
5. Type a value from **1 - 100** in the*% utilization* field. When throughput reaches the specified percentage of port capacity, a threshold alert occurs.
6. Type the *Notification Interval*, in minutes, for the threshold. This is the time during which throughput is measured and threshold notifications can occur. The valid range is **5 - 70560** minutes.

7. Use one of the following options to set a rule for the threshold.
    a. Select *If the threshold is ever exceeded* option to specify that an alert occur when the% *utilization* is reached. The valid range is **1** to the interval set in the step number 8.
    b. Select *If the threshold is exceeded for* option and type the cumulative minutes for which the% *utilization* should exist during the notification interval before an alert is generated.
8. Select *Port List* and use the *E Port*, *F Port* or *Selected Port* option to generate an alert for the configured ports. To select all port numbers in the *Selected Port* table, click the *Set All* button.
9. Select the *Port Type* or *Port List* radio button.
    - Select the *Port Type* radio button, then the *E_Ports*, *F_Ports*, or *FL_Ports* radio button to cause an alert to be generated for the configured port.
    - Select *Port List* to configure individual ports by clicking the check box adjacent to each port number. Select *Set All Ports* to place a check mark adjacent to all port numbers.
10. Click *OK*. This closes the window. The new alert is listed in the *Configure Threshold Alerts* window.
11. Click *OK* after selecting the new alert.

Enable EFCM Basic Edition and Telnet access

Follow the procedure in this section to enable EFCM Basic Edition interface and Telnet access through the maintenance port.

To enable EFCM Basic Edition interface and Telnet access through the maintenance port using the Element Manager, use the following steps:

1. Select *Authentication* from the *Security* menu (*Security>Authentication*). The *Configure Authentication* window appears.
2. Select *Enable Web Server/Enable Telnet Access* in the window.
3. Click *Add* to add users who will be permitted to have EFCM Basic Edition interface / Telnet access. The Add/Edit user window appears.

4. Type the *User ID* and *Password* of the user to be added. Confirm the password in the *Retype* field. Click *OK* to return to the *Configure Authentication* Window.
5. Click *Apply*. The *Security Change Confirmation Status - Users* window appears.
6. Click *Start* to apply the settings.

Configure, enable, and test e-mail notification

Follow the procedures in this section to configure, enable, and test e-mail and simple mail transfer protocol (SMTP) addresses to receive event notifications. Configuration and test are performed at the SAN management application. E-mail notification is enabled at the Element Manager application.

To configure, enable and test e-mail notification using the SAN Management application (EFCM), use the following steps:

1. Select *Email* from the *Monitor* menu (Monitor>*Event Notification>Email)*. The *Email Event Notification Setup* dialog box appears (Figure 42).

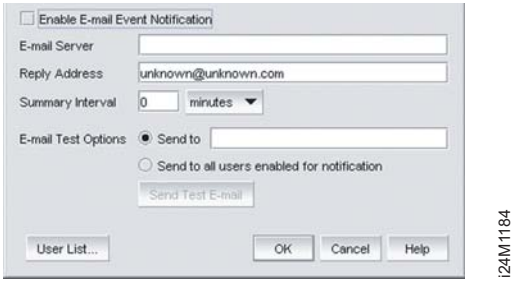


Figure 42 Email Event Notification Setup dialog box

2. Select the *Enable Email Event Notification* check box to enable e-mail transmission to configured addresses.
3. Type the IP address or DNS host name of the SMTP server in the *E-mail Server* field.
4. Type the e-mail address to which replies should be sent in the *Reply Address* field.

5. Type the length of time the application should wait between notifications in the *Summary Interval* field. Choose **seconds**, **minutes**, or **hours** from the associated drop-down list.
6. Click *User List* to specify users for notification. The *EFCM Server Users* dialog box appears.
7. Enable (check) the check box in the *Email* column to enable notification for a user. Click *OK* to close the *EFCM Server Users* dialog box.
8. Select the *Send to* radio button (and type recipient IP addresses in the adjacent field) in the *E-mail Test Options* field or select the *Send to all users enabled for notification* radio button.
9. Click *Send Test Email*. A test message is sent to the configured recipients.
10. Click *OK* to save the information and close the dialog box.

NOTE: Select *Enable E-Mail Notification* from the *Maintenance* menu in the Element Manager. A check mark is displayed to indicate that e-mail notification for the product is enabled.The enable function must be activated for each product through the Element Manager application.

Configure and enable Ethernet events

Follow the procedures in this section to configure and enable Ethernet events. An Ethernet event is recorded (after a user-specified time interval) when the switch-to-management server communication link drops.

To configure and enable Ethernet events using the SAN management application (EFCM), use the following steps:

1. Select *Ethernet Event* from the *Monitor* menu in the EFCM main window. The *Configure Ethernet Events* dialog box appears.
2. Enable (check) the *Enable Ethernet Events* check box.
3. Type a value between **10 - 120** minutes in the *Ethernet Timeout* field,
4. Click *OK* to close the dialog box.

Configure, enable, and test call-home event notification

Telephone numbers and other information for the call-home feature are configured through the Windows dial-up networking application. Refer to *Task 10: Configure the call-home feature (optional)* for configuration instructions.

To configure, enable, and test call-home event notification using the SAN management application (EFCM), use the following steps:

NOTE: The call-home feature may not be available if the EFCM Lite application is installed on a customer-supplied platform.

1. Select *Call Home* from the *Monitor* menu *(Monitor>Event Notification>Call Home)* in the EFCM main window. The *Call Home Event Notification Setup* dialog box appears.
2. Enable (check) the *Enable Call Home Event Notification* check box.

   NOTE: The enable function must be activated for each product through the Element Manager application.

3. Click *Send Test*. A call-home test message is sent.
4. Click *OK* to close the dialog box.
5. Select *Enable Call Home Notification* from the *Maintenance* menu. A check mark appears to indicate call-home event notification is enabled.

Configure security

This section describes optional product security features configured through the SAN management or Element Manager applications. The enhanced SANtegrity PFE key must be installed. Refer to *Install PFE keys (optional)* for instructions.

The optional product security features include:

- **SANtegrity authentication -** Select *Authentication* from the *Configure* menu in the Element Manager application. The *Configure Authentication* dialog box appears. It has five tabs using which you can configure the following optional authentication features.
  - **Users -** Configure password-protected administrator and operator access to the SAN management and Element Manager applications.
  - **Software -** Configure CHAP-controlled management interface access (out-of-band and inband) to the product.
  - **Devices -** Configure a CHAP secret authentication sequence for nodes (devices) attached to the product through E_Ports or N_ports.
  - **IP Access Control -** Configure a list of device IP addresses or a range of device IP addresses authorized to communicate with the product.
  - **RADIUS Servers -** Configure RADIUS servers. A RADIUS server stores and authenticates passwords and CHAP secrets.
- **Enterprise Fabric Mode -** Select *Enterprise Fabric Mode* option from the *Configure* menu (*Configure>Enterprise Fabric Mode*) in EFCM to enable or disable EFM. Fabric binding is activated when EFM is enabled.
- **Fabric binding -** Select *Fabric Binding* from the *Configure* menu (*Configure>Fabric Binding*) to lock parameters of a fabric in accordance with the user configuration. Fabric binding creates a membership list of element (director or switch) Domain_IDs and WWNs that can communicate with the product.
- **Switch binding -**
  - Select *Change State* from the *Security* menu (*Security>Switch Binding>Change State*) to enable Switch Binding and the port type to which it applies (E, F or all).
  - Select *Membership List* from the *Security* menu (*Security>Switch Binding>Membership List*) in EFCM to create a membership list of node (device) WWNs that can attach to the product. The specified connection policy restricts product access through E_Ports, F_Ports, or in general (all ports).

To configure optional features, refer to the *EFC Manager Software Release 8.7 User Manual* (620-000170) for instructions.

Configure interswitch links

This section describes optional ISL performance features configured through the SAN management or Element Manager applications.

The optional ISL performance features that can be configured using EFCM or Element Manager include:

- **OpenTrunking** - Use the *OpenTrunking* option from the *Configure* menu (*Configure>Open Trunking*) in the Element Manager to optimize ISL bandwidth. The feature monitors data rates (congestion and BB_Credit starvation) through multiple ISLs and load balances traffic (from congested to uncongested links) accordingly.
- **Preferred path -** Use the *Preferred Path* option from the *Configure* menu (*Configure>Preferred Path*) in the Element Manager to specify and configure one or more ISL data paths between multiple fabric elements. At each fabric element, a preferred path consists of a source port, exit port, and destination Domain_ID.
- **Port fencing -** Use the *Port Fencing* option from the *Configure* menu (*Configure>Port Fencing*) in EFCM to minimize ISLs that bounce (repeatedly attempt to establish a connection), causing disruptive fabric rebuilds. Fencing defines a bounce threshold that when reached, automatically blocks the disruptive E_Port.

For more information configuring optional features, refer to the *EFC Manager Software Release 8.9 User Manual* (620-000170) for instructions.

If no additional options or features are to be configured, go to *Task 19: Back up configuration data*.

Task 19: Back up configuration data

For the Sanavigator application, critical configuration data is stored on the management server hard drive in the following directories:

- **C:\Program Files\SANavigator 4.2\CallHome**
- **C:\Program Files\SANavigator 4.2\Client**
- **C:\Program Files\SANavigator 4.2\Server**.

For the EFCM application, critical configuration data is stored on the management server hard drive in the following directories:

- **C:\Program Files\EFCM 8.7\CallHome**
- **C:\Program Files\EFCM 8.7\Client**
- **C:\Program Files\EFCM 8.7\Server.**

The server is configured to automatically mirror the contents of these directories to the CD-RW drive anytime directory contents change or the server is rebooted. The directories contain all SAN management configuration data, log files, firmware versions, call-home and other configuration data; and are used to restore the server operating environment in case of hard drive failure.

The server does not back up Windows operating system data, such as user names, passwords, date and time, and network information. This information was recorded while performing installation tasks, and verified while performing *Task 13: Record or verify server restore information*.

To back up server configuration data and create a base restore CD:

1. Insert a blank rewritable CD into the CD-RW drive and format the CD:
   a. Locate the *InCD* icon (**1**) at the right side of the task bar on your Windows desktop (Figure 43). The icon is indicated by a red down arrow.

Figure 43 InCD icon (unformatted CD)

   b. Right-click the icon and select *Format (F)*. The first window of the *InCD* wizard appears.
   c. Click *Next* to proceed to the second window of the *InCD* wizard. Use default parameters displayed at each window, and click *Next* and *Finish* as appropriate to complete the CD formatting task.

When the rewritable CD is formatted, the red down arrow associated with the *InCD* icon changes to a green up arrow.

2. Back up the product configuration file to the server. For instructions, refer to *Back up configuration*.
3. Close the Element manager application and return to the SAN management application.
4. Close the SAN management application by selecting *Shutdown* from the *SAN* menu. An *EFCM Message* dialog box appears. Click *Yes* to close the application.
5. Reboot the server to cause directory contents to be written to the blank CD:
   a. At the Windows desktop, click *Start* at the left side of the task bar (bottom of the desktop), then select *Shut Down*. The *Shut Down Windows* dialog box appears.
   b. Select the *Restart* option from the list box and click *OK*. The server powers down and restarts. During the reboot process the LAN connection between the server and browser-capable PC drops momentarily, and the TightVNC viewer displays a network error.
   c. After the management server reboots, click *Login again*. The *VNC Authentication* screen appears.
   d. Type the default password and click *OK*. The *Welcome to Windows* dialog box appears.

      NOTE: The default TightVNC viewer password is **password.**

   e. Click the **Send Ctrl-Alt-Del** button at the top of the window to log on to the server desktop. The *Log On to Windows* dialog box appears.

      NOTE: Do not simultaneously press the **Ctrl**, **Alt**, and **Delete** keys. This action logs the user on to the browser-capable PC, not the server.

   f. Type the default Windows user name and password and click *OK*. The server's Windows desktop opens and the *EFCM Log In* dialog box appears.

NOTE: The default Windows user name is **Administrator** and the default password is **password**. Both are case-sensitive.

g. Type the SAN management application default user ID and password and select a server or IP address from the *Network Address* drop-down list.

NOTE: The default user ID is **Administrator** and the default password is **password.** Both are case-sensitive.

6. Click *Login*. The application opens and the EFCM main window appears.
7. Remove the base restore CD from the CD-RW drive and store in a safe location. Insert a blank rewritable CD into the CD-RW drive and format the CD. Refer to step 1 for formatting instructions.
8. Go to *Task 20: Cable Fibre Channel ports*.

Task 20: Cable Fibre Channel ports

Follow the procedures in this section to cable Fibre Channel ports and connect devices.

To cable Fibre Channel ports and connect devices, use the following steps:

1. Route fiber-optic jumper cables from customer-specified Fibre Channel devices, FC-AL devices, or fabric elements to product ports.
2. Connect device cables to SFP optical port transceivers as directed by the customer.
3. Perform one of the following:
   - If the product is installed on a table or desktop, bundle and secure Fibre Channel cables as directed by the customer.
   - If the product is installed in a customer-supplied equipment rack, bundle Fibre Channel cables from the product and other equipment (groups of 16 maximum), and secure them as directed by the customer.

- If the product is installed in a Fabricenter equipment cabinet, bundle Fibre Channel cables from the product and other equipment (groups of 16 maximum), and secure them in the cable management area at the front-left side of the cabinet.

Task 21: Configure zoning (optional)

Follow the instructions in this section to configure the zoning options for the product.

To configure zones and zone sets for the product, use the following instructions:

- **Zone -** A zone is a group of devices that can access each other through port-to-port connections. Devices in the same zone can recognize and communicate with each other; devices in different zones cannot.
- **Zone set -** A zone set is a group of zones that is activated or deactivated as a single entity across all managed products in either a single switch or a multiswitch fabric. Only one zone set can be active at one time.

The following naming conventions apply to zones and zone sets:

- All names must be unique and may not differ by case only. For example, **zone-1** and **Zone-1** are both valid individually, but are not considered unique.
- The first character of a zone set name must be a letter (**A** through **Z** or **a** through **z**).
- A zone set name cannot contain spaces.
- Valid characters are alphanumerics and the caret (**^**), hyphen (**-**), underscore (_), or dollar (**$**) symbols.
- A zone set name can have a maximum of 64 characters.

If the installation is performed from the EFCM Basic Edition interface, refer to the *EFCM Basic Edition User Manual* (620-000240) for instructions.

If the installation is performed from the management server, refer to the *EFC Manager Software Release 8.7 User Manual* (620-000170) for instructions.

Task 22: Connect product to a fabric element (eptional)

To provide fabric-attached Fibre Channel connectivity for devices connected to the product, connect the product to an expansion port (E_Port) of a fabric element (switch or director). Any switch can be used to form this ISL.

To connect the product to a fabric element and create an ISL use the following steps:

1. Ensure that the fabric element is accessible by the EFCM Basic Edition interface or defined to the SAN management application. If the fabric element must be defined, refer to the appropriate switch or director installation manual for instructions.
2. Ensure that the preferred domain ID for the product is unique and does not conflict with the ID of another switch or director participating in the fabric.
   - — If the domain ID must be changed from the EFCM Basic Edition, refer to *Task 4: Configure product using EFCM Basic (optional)*.
   - — If the domain ID must be changed from the management server, refer to *Task 18: Configure the Element Manager application*.
3. Ensure that R_A_TOV and E_D_TOV values for the product are identical to the values for all switches or directors participating in the fabric.
   - — If the values must be changed from the EFCM Basic Edition, refer to *Task 4: Configure product using EFCM Basic (optional)*.
   - — If the values must be changed from the management server, refer to *Task 18: Configure the Element Manager application*.
4. Route a multimode or singlemode fiber-optic cable (depending on the type of transceiver installed) from a customer-specified E_Port of the fabric element to the front of the product.
5. Connect the fiber-optic cable to a product port as directed by the customer.
6. If the product is managed through the management server, go to step 7. If the product is managed through EFCM Basic Edition:
   a. Select *Port List* from the *Product* menu at any view. The *Port List* view appears.

b. At the *Port List* view, click the physical port number of the fabric ISL (connected in step 5) in the *Port* column. Physical properties for the port appear in the lower panel of the view.

c. Ensure that the *Operational State* field displays **Online** and the *Reason* field displays **N/A** or is blank. If an ISL segmentation or other problem is indicated, go to *MAP 0000: Start MAP* to isolate the problem. If no problems are indicated, installation tasks are complete.

7. Right-click the product icon in the EFCM physical map; select *Element Manager* from the pop-up menu
8. Click the *Hardware* tab. The *Hardware* view (Figure 31) appears.
9. Double-click the graphical port connector used for the fabric ISL (connected in step 5). The *Port Properties* dialog box appears.
10. Ensure that the *Link Incident* field displays **None**, the *Operational State* field displays **Online**, and the *Reason* field displays **N/A** or is blank. If an ISL segmentation or other problem is indicated, go to *MAP 0000: Start MAP* to isolate the problem. If no problems are indicated, installation tasks are complete.

Chapter 3: Maintenance analysis procedures

This chapter describes maintenance analysis procedures (MAPs) used by service representatives to fault isolate switch problems or failures . MAPs consist of step-by-step procedures that provide information to interpret system events, isolate a failure to a single part, remove and replace the failed part, and verify product operation.

Factory defaults

Table 5 lists factory defaults for product passwords (customer and maintenance level), and the product's Internet Protocol (IP) address, subnet mask, and gateway address.

Table 5 Factory-set defaults

Item	Default
Customer password	password
Maintenance password	level-2
IP address	10.1.1.10
Subnet mask	255.0.0.0
Gateway address	0.0.0.0

Quick start

Table 6 lists and summarizes MAPs. Fault isolation normally begins at *MAP 0000: Start MAP*.

Table 6 MAP summary

MAP	Page
MAP 0000: Start MAP	104
MAP 0100: Power distribution analysis	109
MAP 0200: POST failure analysis	111

© Copyright IBM Corp. 2006

Table 6 MAP summary (Continued)

MAP	Page
MAP 0300: Loss of server communication	113
MAP 0400: Part failure analysis	123
MAP 0500: Port failure or link incident analysis	126
MAP 0600: Fabric or ISL problem analysis	138

Table 7 lists event codes, corresponding MAP references, and provides a quick start guide if an event code is readily available.

Table 7 Event codes versus maintenance action

Event code	Explanation	Action
011	Login Server database invalid.	Go to MAP 0600.
021	Name Server database invalid.	Go to MAP 0600.
031	SNMP request received from unauthorized community.	Add a community name at the Element Manager.
051	Management Server database invalid.	Go to MAP 0600.
061	Fabric Controller database invalid.	Go to MAP 0600.
062	Maximum interswitch hop count exceeded.	Go to MAP 0600.
063	Remote switch has too many ISLs.	Go to MAP 0600.
064	ESS response from indicated domain ID not received after maximum tries.	No action required.
070	E_Port is segmented.	Go to MAP 0600.
071	Switch is isolated.	Go to MAP 0600.
072	E_Port connected to unsupported switch.	Go to MAP 0600.
073	Fabric initialization error.	Go to *Collect maintenance data*. (EFCM Basic) or *Collect maintenance data* (Element Manager).
074	ILS frame delivery error threshold exceeded.	Go to *Collect maintenance data*. (EFCM Basic) or *Collect maintenance data* (Element Manager).
075	E_Port segmentation recovery.	No action required.

Table 7 Event codes versus maintenance action (Continued)

Event code	Explanation	Action
080	Unauthorized worldwide name.	Go to MAP 0500.
081	Invalid attachment.	Go to MAP 0500
082	Port fenced.	Go to MAP 0600.
083	Port set to inactive state.	Go to MAP 0500
120	Error detected while processing system management command.	Go to *Collect maintenance data*. (EFCM Basic) or *Collect maintenance data* (Element Manager).
121	Zone set activation failed - zone set too large.	Reduce size of zone set and retry.
140	Congestion detected on an ISL.	Go to MAP 0600.
141	Congestion relieved on an ISL.	No action required.
142	Low BB_Credit detected on an ISL.	Go to MAP 0600.
143	Low BB_Credit relieved on an ISL.	No action required.
150	Fabric merge failure.	Go to MAP 0600.
151	Fabric configuration failure.	Go to *Collect maintenance data*. (EFCM Basic) or *Collect maintenance data* (Element Manager).
200	Power supply AC voltage failure.	Go to MAP 0100.
201	Power supply DC voltage failure.	Go to MAP 0100.
203	Power supply AC voltage recovery.	No action required.
204	Power supply DC voltage recovery.	No action required.
206	Power supply removed.	Replace CRU.
207	Power supply installed.	No action required.
300	Cooling fan propeller failed.	Go to MAP 0400.
301	Cooling fan propeller failed.	Go to MAP 0400.
302	Cooling fan propeller failed.	Go to MAP 0400.
303	Cooling fan propeller failed.	Go to MAP 0400.
304	Cooling fan propeller failed.	Go to MAP 0400.
305	Cooling fan propeller failed.	Go to MAP 0400.

Table 7 Event codes versus maintenance action (Continued)

Event code	Explanation	Action
310	Cooling fan propeller recovered.	No action required.
311	Cooling fan propeller recovered.	No action required.
312	Cooling fan propeller recovered.	No action required.
313	Cooling fan propeller recovered.	No action required.
314	Cooling fan propeller recovered.	No action required.
315	Cooling fan propeller recovered.	No action required.
370	Cooling fan status polling temporarily disabled.	Go to MAP 0400.
400	Power-up diagnostic failure.	Go to MAP 0200.
410	Switch reset.	No action required.
411	Firmware fault.	Go to MAP 0200.
412	CTP watchdog timer reset.	Go to *Collect maintenance data*. (EFCM Basic) or *Collect maintenance data* (Element Manager).
421	Firmware download complete.	No action required.
423	CTP firmware download initiated.	No action required.
426	Multiple ECC single-bit errors occurred.	Go to MAP 0400.
433	Non-recoverable Ethernet fault.	Go to MAP 0400.
440	Embedded port hardware failed.	Go to MAP 0400.
442	Embedded port anomaly detected.	No action required.
445	ASIC detected a system anomaly.	No action required.
453	New feature key installed.	No action required.
506	Fibre Channel port failure.	Go to MAP 0500.
507	Loopback diagnostics port failure.	Go to MAP 0500.
508	Fibre Channel port anomaly detected.	No action required.
510	Optical transceiver hot-insertion initiated.	No action required.
512	Optical transceiver nonfatal error.	Go to MAP 0500.

Table 7 Event codes versus maintenance action (Continued)

Event code	Explanation	Action
513	Optical transceiver hot-removal completed.	No action required.
514	Optical transceiver failure.	Go to MAP 0500
515	Optical digital diagnostics warning threshold exceeded.	Go to MAP 0500.
516	Optical digital diagnostics alarm threshold exceeded.	Go to MAP 0500.
523	FL_Port open request failed.	No action required.
524	No AL_PA acquired.	No action required.
525	FL_Port arbitration timeout.	No action required.
581	Implicit incident.	Go to MAP 0500.
582	Bit error threshold exceeded.	Go to MAP 0500.
583	Loss of signal or loss of synchronization.	Go to MAP 0500.
584	Not operational primitive sequence received.	Go to MAP 0500.
585	Primitive sequence timeout.	Go to MAP 0500.
586	Invalid primitive sequence received for current link state.	Go to MAP 0500.
810	High temperature warning (CTP thermal sensor).	Go to MAP 0400.
811	Critically hot temperature warning (CTP thermal sensor).	Go to MAP 0400.
812	CTP card shutdown due to thermal violations.	Go to MAP 0400.
850	Switch shutdown due to CTP thermal violations.	Go to MAP 0400.

MAP 0000: Start MAP

This MAP describes initial fault isolation beginning at the:

- Failed product.
- Browser-capable PC with Internet connectivity to the firmware-resident Enterprise Fabric Connectivity Manager (EFCM) Basic Edition interface.
- Rack-mount management server running storage area network (SAN) management and Element Manager applications.
- Product-attached open systems interconnection (OSI) host console.

1

Prior to fault isolation, have the following available:

- A system configuration drawing or planning worksheet that includes the location of the product, management interface, other IBM products, and device connections.
- The internet protocol (IP) address, gateway address, and subnet mask for the product reporting the problem.
- User IDs and passwords.

Continue to the next step.

2

Ensure the product is connected to facility power. Inspect the product for indications of being powered on, such as:

- An illuminated **PWR** LED (green) or **ERR** LED (amber).
- Illuminated LEDs adjacent to Fibre Channel ports.
- Noise and airflow from cooling fans.

Is the product powered on?

YES	NO
↓	A power distribution problem is indicated. Go to *MAP 0100: Power distribution analysis*. **Exit MAP.**

3

At the failed product, inspect the amber **ERR** LED and amber LEDs associated Fibre Channel ports and CRUs.

Are any amber LEDs illuminated?

NO **YES**

↓ A CRU failure, power-on self-test (POST) failure, link incident, interswitch link (ISL) problem, fenced E_Port, or segmented E_Port is indicated. To obtain event codes that identify the failure, **go to step 10.**

4

Is the product management interface (browser PC, management server, or OSI host console) powered on and operational?

NO **YES**

↓ **Go to step 7.**

5

Power on the management interface platform and launch the associated management application:

- **EFCM Basic Edition -** Refer to *Task 4: Configure product using EFCM Basic (optional)* for instructions.
- **SAN management application -** Refer to *Task 6: Configure server password and network addresses* and *Access the management server desktop* for instructions.
- **OSI host console -** Refer to documentation supplied with the host system for instructions.

Was the maintenance action successful?

NO **YES**

↓ **Go to step 7.**

6

Inspect the management interface for communication link failure. Observe one of the following:

- A **Page cannot be found**, **Unable to locate the server, HTTP 404 - file not found**, or similar message (browser PC).

- The icon representing the product displays a grey square with an exclamation mark (SAN management application).
- A grey square at the alert panel, a No Link status and reason, and no visible product CRUs (Element Manager *Hardware View*).

Was a failure indication observed?

NO **YES**

↓ Communication between the product and management interface failed. Go to *MAP 0300: Loss of server communication*. **Exit MAP.**

Perform a data collection and contact the next level of support. Refer to *Collect maintenance data* (EFCM Basic Edition) or *Collect maintenance data* (Element Manager). **Exit MAP.**

7

Inspect product status at the management interface:

a. For the product reporting the problem:

   — **EFCM Basic Edition -** Select *Hardware* from the *Product* menu at any view. The *Hardware View* displays.

   — **SAN management application -** At the physical map, right-click the status icon for the product reporting the problem and select *Element Manager* from the pop-up menu. The Element Manager opens and the *Hardware View* displays.

   — **OSI host console - Go to step 9.**

b. Inspect the status symbol associated with the product. A yellow triangle (attention indicator) indicates the product is operating in degraded mode. A red diamond (failure indicator) indicates the product is not operational.

c. Inspect simulated Fibre Channel ports for a yellow triangle (attention indicator) that overlays the CRU graphic.

d. Inspect simulated CRUs for a blinking red and yellow diamond (failed CRU indicator) that overlays the CRU graphic.

Is a failure indicated?

NO **YES**

↓ A CRU failure, power-on self-test (POST) failure, link incident, interswitch link (ISL) problem, fenced E_Port, or segmented E_Port is indicated. To obtain event codes that identify the failure, **go to step 10.**

8

A link incident may have occurred, but the LIN alerts option is not enabled and the yellow triangle (attention indicator) does not appear. Inspect the *Link Incident Log*:

a. For the product reporting the problem:

- **EFCM Basic Edition -** Select *Link Incident* from the *Logs* menu at any view. The *Link Incident Log* displays.
- **Element Manager -** Select *Link Incident Log* from the *Logs* menu at any view. The *Link Incident Log* displays.

b. If a link incident occurred, the port number is listed with one of the following messages.

- **Link interface incident - implicit incident.**
- **Link interface incident - bit-error threshold exceeded.**
- **Link failure - loss of signal or loss of synchronization.**
- **Link failure - not-operational primitive sequence (NOS) received.**
- **Link failure - primitive sequence timeout.**
- **Link failure - invalid primitive sequence received for the current link state.**

Did a listed message appear?

NO **YES**

↓ A Fibre Channel link incident is indicated. Go to *MAP 0500: Port failure or link incident analysis*. **Exit MAP.**

Perform a data collection and contact the next level of support. Refer to *Collect maintenance data* (EFCM Basic Edition) or *Collect maintenance data* (Element Manager). **Exit MAP.**

9

If an incident occurs on the Fibre Channel link between the product and attached OSI server, a link incident record is generated and sent to the server console using the reporting procedure defined in T11/99-017v0.

Was a link incident record generated and sent to the OSI server?

NO **YES**

↓ A Fibre Channel link incident is indicated. Go to *MAP 0500: Port failure or link incident analysis*. **Exit MAP.**

Perform a data collection and contact the next level of support. Refer to *Collect maintenance data* (EFCM Basic Edition) or *Collect maintenance data* (Element Manager). **Exit MAP.**

10

Inspect the *Event Log* to obtain failure reason codes:

a. For the product reporting the problem:
   - **EFCM Basic Edition -** Select *Event* from the *Logs* menu at any view. The *Event Log* displays.
   - **Element Manager -** Select *Event Log* from the *Logs* menu at any view. The *Event Log* displays.

b. Record the event code and associated date, time, and severity (*Informational*, *Minor*, *Major*, or *Severe*).

c. If multiple event codes are found, record all codes and severity levels. Record the date, time, and sequence, and determine if all codes are related to the reported problem. Begin fault isolation with the most recent event code with the highest severity level. Other codes may accompany this event code, or may indicate a normal indication after a problem is recovered.

Were one or more event codes found?

NO **YES**

↓ **Go to Table 7** to obtain event codes. **Exit MAP.**

Return to step 1 and perform fault isolation again. If this is the second time at this step, perform a data collection and contact the next level of support. Refer to *Collect maintenance data* (EFCM Basic Edition) or *Collect maintenance data* (Element Manager).
Exit MAP.

MAP 0100: Power distribution analysis

This MAP describes fault isolation for the product power distribution system, including defective AC power cords or redundant power supplies. One or more of the following indicate a failure:

- Failure of the product to power on.
- Event code **200** or **201** observed at the *Event Log* (EFCM Basic Edition or Element Manager interface).

1

Ensure the product is connected to facility power. Inspect the product for indications of being powered on, such as:

- An illuminated **PWR** LED (green) or **ERR** LED (amber).
- Illuminated LEDs adjacent to Fibre Channel ports.
- Noise and airflow from cooling fans.

Is the product powered on?

YES **NO**

↓ A power distribution problem is indicated. **Go to step 4.**

2

Table 8 lists event codes, explanations, and MAP steps.

Table 8 MAP 100 event codes

Event code	Explanation	Action
200	Power supply AC voltage failure.	Go to step 3.
201	Power supply DC voltage failure.	Go to step 3.

3

As indicated by visual inspection or event code **200** or **201**, one or both power supplies failed and must be removed and replaced. Refer to *Field-replaceable unit: Redundant power supply*.

- The procedure is concurrent and performed while the product is operational.

- If multiple fan failures caused a thermal shutdown, connect the product to facility AC power after power supply(s) are replaced.
- Perform a data collection as part of removal and replacement. Refer to *Collect maintenance data* (EFCM Basic Edition) or *Collect maintenance data* (Element Manager).

NOTE: Do not remove a power supply unless a replacement part is available. To avoid product overheating, a removed power supply must be replaced within five minutes.

Was the maintenance action successful?

NO **YES**

↓ The product is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

4

Inspect and verify facility power is within specifications:

- One single-phase connection for each power supply.
- Input power between 100 and 240 VAC, at least 5 amps.
- Input frequency between 47 and 63 Hz.

Is facility power within specifications?

YES **NO**

↓ Ask the customer to correct the facility power problem. When corrected, **continue to the next step.**

5

One or both power supplies are disconnected from facility power, improperly installed, or failed. Verify power supplies are connected to facility power.

a. Ensure AC power cords are connected to the rear of the switch and facility power receptacles. If not, connect power cords as directed by the customer.

b. Ensure facility circuit breakers are on. If not, ask the customer to set breakers on.

c. Ensure AC power cords are not damaged. If damaged, replace the cords.

Was the maintenance action successful?

NO **YES**

↓ The product is operational. **Exit MAP.**

6

Verify power supply operation.

a. Inspect each power supply to determine if the amber failure LED is illuminated.

b. If an amber LED is illuminated, ensure the indicated power supply is correctly installed and seated. Partially remove and reseat the power supply. Refer to *Field-replaceable unit: Redundant power supply*.

Was the maintenance action successful?

NO **YES**

↓ The product is operational. **Exit MAP.**

A power supply failure is indicated. **Go to step 3.**

MAP 0200: POST failure analysis

This MAP describes fault isolation for a POST failure. The failure indicator is event code **400** or **411** observed at the *Event Log* (EFCM Basic Edition or Element Manager interface).

1

Table 9 lists event codes, explanations, and MAP steps.

Table 9 MAP 200 Event Codes

Event code	Explanation	Action
400	Power-up diagnostic failure.	Go to step 2.
411	Firmware fault.	Go to step 4.

2

As indicated by event code **400**, POST/IPL diagnostics detected a CRU failure.

a. At the *Event Log*, examine the first two bytes of event data.

b. Byte **0** specifies failed CRU. Byte **1** specifies the slot number of the failed part (**00** for nonredundant, **00** or **01** for redundant) as listed in Table 10.

Table 10 MAP 200 Byte 0 CRU Codes

Byte 0	Failed CRU	Action
02	CTP card.	Replace the switch. **Exit MAP.**
05	Fan module.	Go to step 3.
06	Power supply.	Go to step 3.

3

A fan module or power supply failed POSTs and the power supply (containing the fan, if applicable) must be removed and replaced. Refer to *Field-replaceable unit: Redundant power supply*.

- The procedure is concurrent and performed while the product is operational.
- If multiple fan failures caused a thermal shutdown, connect the product to facility AC power after power supply(s) are replaced.
- Perform a data collection as part of the removal and replacement. Refer to *Collect maintenance data* (EFCM Basic Edition) or *Collect maintenance data* (Element Manager).

NOTE: Do not remove a power supply unless a replacement part is available. To avoid product overheating, a removed power supply must be replaced within five minutes.

Was the maintenance action successful?

NO **YES**

↓ The product is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

4

As indicated by event code **411**, POST/IPL diagnostics detected a firmware failure and performed an online dump. All Fibre Channel ports reset after failure and devices momentarily logout, login, and resume operation. Perform a data collection and contact the next level of support. Refer to *Collect maintenance data* (EFCM Basic Edition) or *Collect maintenance data* (Element Manager). **Exit MAP.**

MAP 0300: Loss of server communication

This MAP describes fault isolation for the product to browser PC Internet connection (EFCM Basic Edition interface) or the product to management server LAN connection. One or more of the following indicate a failure:

- A **Page cannot be found**, **Unable to locate the server**, **HTTP 404 - file not found**, or similar message (browser PC).
- The icon representing the product displays a grey square with an exclamation mark (SAN management application).
- A grey square at the alert panel, a **No Link** status and reason, and no visible product CRUs (Element Manager *Hardware View*).

NOTE: Upon restart, it may take up to five minutes for the management interface logical connection to activate. This delay is normal.

1

The following product management interface failed:

- EFCM Basic Edition (browser PC). **Go to step 2.**
- SAN management or Element Manager application (management server). **Go to step 5.**

2

A **Page cannot be found**, **Unable to locate the server**, **HTTP 404 - file not found**, or similar message appears at the browser PC, indicating the PC cannot communicate with the product because:

- The product-to-PC Internet link could not be established.

- AC power distribution for the product failed or AC power was disconnected.
- The product CTP card failed.

Continue to the next step.

3

Ensure the product is connected to facility power. Inspect the product for indications of being powered on, such as:

- An illuminated **PWR** LED (green) or **ERR** LED (amber).
- Illuminated LEDs adjacent to Fibre Channel ports.
- Noise and airflow from cooling fans.

Is the product powered on?

YES **NO**

↓ A power distribution problem is indicated. Go to *MAP 0100: Power distribution analysis*. **Exit MAP.**

4

A product-to-PC link problem (Internet too busy or IP address typed incorrectly) or an Ethernet port failure is indicated.

a. Wait approximately five minutes, then attempt to login to the product.

b. At the *Netsite* field (Netscape Navigator) or *Address* field (Internet Explorer), type **http://xxx.xxx.xxx.xxx**, where **xxx.xxx.xxx.xxx** is the product IP address obtained in *MAP 0000: Start MAP*. The *Username and Password Required* dialog box appears.

c. Type the user name and password obtained in *MAP 0000: Start MAP* and click *OK*. If the EFCM Basic Edition interface does not open, wait five minutes and perform this step again.

Is the EFCM Basic Edition interface operational?

NO **YES**

↓ The Internet connection is restored. **Exit MAP.**

Failure of the Ethernet port is indicated. Replace the switch.
Exit MAP.

5

A status icon (grey square with yellow exclamation mark) appears at the SAN management application, indicating the management server cannot communicate with the product because:

- The server-to-PC Internet link could not be established.
- AC power distribution for the product failed or AC power was disconnected.
- The product CTP card failed.

Continue to the next step.

6

Ensure the product is connected to facility power. Inspect the product for indications of being powered on, such as:

- An illuminated **PWR** LED (green) or **ERR** LED (amber).
- Illuminated LEDs adjacent to Fibre Channel ports.
- Noise and airflow from cooling fans.

Is the product powered on?

YES **NO**

↓ A power distribution problem is indicated. Go to *MAP 0100: Power distribution analysis*. **Exit MAP.**

7

At the SAN management application's physical map, right-click the status icon for the product reporting the problem and select *Element Manager* from the pop-up menu. The Element Manager opens and the *Hardware View* displays:

- A grey square appears at the alert panel.
- No product CRUs are visible.
- The *Status* table is yellow, the *Status* field displays **No Link**, and the **Reason** field displays an error message listed in Table 11.

Table 11 MAP 300 error messages

Error message	Action
Never connected.	Go to step 8.
Link timeout.	Go to step 8.
Protocol mismatch.	Go to step 15.
Duplicate session.	Go to step 18.
Unknown network address.	Go to step 21.
Incorrect product type.	Go to step 23.

8

Transmit or receive errors for the Ethernet adapter exceeded a threshold, the link was not connected, or the link timed out. A problem with the Ethernet cable, Ethernet hub(s), or other LAN-attached device is indicated. Verify the product is connected to the management server through one or more Ethernet hubs:

a. Ensure an RJ-45 Ethernet cable connects the product to a hub. If not, connect the cable as directed by the customer.

b. Ensure an RJ-45 Ethernet cable connects the management server to a hub. If not, connect the cable as directed by the customer.

c. Ensure Ethernet cables are not damaged. If damaged, replace the cables.

Was the maintenance action successful?

NO **YES**

↓ The management server connection is restored. **Exit MAP.**

9

Does the configuration use multiple daisy-chained Ethernet hubs?

YES **NO**

↓ **Go to step 11.**

10

Verify hubs are correctly daisy-chained.

a. **Top hub -** As shown in Figure 44 (**1**), ensure an RJ-45 Ethernet cable connects to port **24** and the medium-dependent interface (MDI) switch is set to **MDI** (in).

b. **Middle hub -** As shown in Figure 44 (**2**), ensure the cable from the top hub connects to port **12,** the cable from the bottom hub connects to port **24**, and the MDI switch is set to **MDI** (in).

c. **Bottom hub -** As shown in Figure 44 (**3**), ensure the cable from the middle hub connects to port **12** and the MDI switch is set to **MDIX** (out).

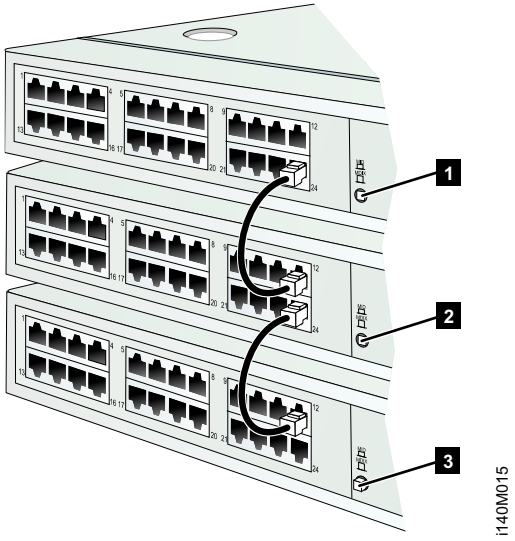


Figure 44 Daisy-Chained Ethernet Hubs

Was the maintenance action successful?

NO **YES**

↓ The management server connection is restored. **Exit MAP.**

11

Verify operation of Ethernet hub(s). Inspect each hub for indications of being powered on, such as:

- Green **Power** LED illuminated.
- Green **Status** LEDs illuminated.

Is a failure indicated?

YES **NO**

↓ **Go to step 13.**

12

Remove and replace the Ethernet hub. Refer to supporting documentation for instructions.

Was the maintenance action successful?

NO **YES**

↓ The management server connection is restored. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

13

A problem with LAN-attached device is indicated.

- If the problem is associated with another fabric element or management server, go to *MAP 0000: Start MAP* to isolate the problem for that product. **Exit MAP.**
- If the problem is associated with an unrelated device, inform the customer for problem resolution.

Was the maintenance action successful?

NO **YES**

↓ The management server connection is restored. **Exit MAP.**

14

The Ethernet adapter on the product CTP card reset in response to an error. The connection to the management server terminated briefly, then recovered upon reset. Perform a data collection and contact the next level of support. Refer to *Collect maintenance data* (EFCM Basic Edition) or *Collect maintenance data* (Element Manager). **Exit MAP.**

15

A protocol mismatch occurred because the SAN management application and the product firmware are not at compatible release levels. Recommend that the customer upgrade the downlevel version (software or firmware).

Does the SAN management application require upgrade?

YES **NO**

↓ **Go to step 17.**

16

Upgrade the SAN management application. Refer to *Install or upgrade software*.

Was the maintenance action successful?

NO **YES**

↓ The management server connection is restored. **Exit MAP.**

17

Product firmware upgrade is required. Refer to *Upgrade firmware* (EFCM Basic Edition) or *Upgrade firmware* (Element Manager). Perform a data collection after the upgrade. Refer to *Collect maintenance data* (EFCM Basic Edition) or *Collect maintenance data* (Element Manager).

Was the maintenance action successful?

NO **YES**

↓ The management server connection is restored. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

18

An instance of the SAN management application is open at another management server and communicating with the product (duplicate session). Inform the customer and either:

- Power off the server running the second instance of the application.
- Configure the server running the second instance of the application as a client workstation.

Does the customer want the second server configured as a client?

YES **NO**

↓ Power off the server reporting the **Duplicate Session** problem. **Exit MAP.**

19

Determine the IP address of the management server running the first instance of the SAN management application.

a. After the server powers on and successfully completes POSTs, the LCD panel displays a **Welcome!!** message and continuously cycles through and displays operational information.

b. After a few seconds, the LCD panel displays a **LAN 2: 010.001.001.001** message.

c. Depending on product-to-server LAN connectivity, record the appropriate IP address (**LAN 1** or **LAN 2**).

Continue to the next step.

20

Configure the management server reporting the **Duplicate Session** problem as a client.

a. At the SAN management application, select *Logout* from the *SAN* menu. The application closes and the *Log In* dialog box displays.

b. Type the user ID and password obtained in *MAP 0000: Start MAP*. Both are case sensitive).

c. Type the IP address of the management server running the first instance of the SAN management application in the *Network Address* field.

d. Click *Login*. The application opens and the main window displays.

Was the maintenance action successful?

NO **YES**

↓ The management server connection is restored and the second management server is a client. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

21

The IP address defining the product to the SAN management application is incorrect or unknown and must be verified. An asynchronous RS-232 modem cable and maintenance terminal (desktop or notebook PC) with a Windows-based operating system and RS-232 serial communication software (such as ProComm Plus or HyperTerminal) are required. To verify the IP address:

a. Using a Phillips screwdriver, remove the protective cap from the 9-pin maintenance port at the rear of the chassis. Connect one end of the RS-232 modem cable to the port.

b. Connect the other cable end to a 9-pin serial communication port (**COM1** or **COM2**) at the rear of the maintenance terminal PC.

c. Power on the maintenance terminal. At the Windows desktop, click *Start* at the left side of the task bar. The *Windows Workstation* menu displays.

d. At the *Windows Workstation* menu, sequentially select the *Programs*, *Accessories*, *Communications*, and *HyperTerminal* options. The *Connection Description* dialog box displays.

e. Type a descriptive product name in the *Name* field and click *OK*. The *Connect To* dialog box displays.

f. Ensure the *Connect using* field displays **COM1** or **COM2** (depending on the port connection to the product), and click *OK*. The *COMn Properties* dialog box displays, where *n* is **1** or **2**.

g. Configure *Port Settings* parameters:

   — *Bits per second* - **115200**.

   — *Data bits* - **8**.

   — *Parity* - **None**.

   — *Stop bits* - **1**.

   — *Flow control* - **Hardware** or **None**.

   Click *OK*. The *New Connection - HyperTerminal* window displays.

h. At the **>** prompt, type the user password (default is **password**) and press **Enter**. The password is case sensitive. The *New Connection - HyperTerminal* window displays with software and hardware version information for the product, and a **C >** prompt at the bottom of the window.

i. At the **C >** prompt, type the **ipconfig** command and press **Enter**. The *New Connection - HyperTerminal* window displays with configuration information listed.

j. Record the product IP address.

k. Select *Exit* from the *File* pull-down menu. A HyperTerminal message box appears.

l. Click *Yes*. A second message box appears. Click *No* to exit and close the application.

m. Power off the maintenance terminal and disconnect the modem cable. Replace the protective cap over the maintenance port.

Continue to the next step.

22

Define the product IP address (determined in step 21) to the management server.

a. At the SAN management application, select *Setup* from the *Discover* menu. The *Discover Setup* dialog box displays.

b. Ensure the product to be reconfigured is moved from the *Selected Individual Addresses* list to the *Available Addresses* list. Select (highlight) the product and click *Edit*. The *Address Properties* dialog box displays with the *IP Address* page open.

c. Type the correct product IP address in the *IP Address* field.

d. Move the reconfigured product from the *Available Addresses* list to the *Selected Individual Addresses* list.

e. Click *OK* to save the address, close the dialog box, and redefine the product to the SAN management application.

f. Click *OK* to close the *Discover Setup* dialog box.

Was the maintenance action successful?

NO **YES**

↓ The management server connection is restored. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

23

An incorrect product type is defined to the management server.

a. At the SAN management application, select *Setup* from the *Discover* menu. The *Discover Setup* dialog box displays.

b. Ensure the incorrect product (to be deleted) is moved from the *Selected Individual Addresses* list to the *Available Addresses* list. Select (highlight) the product and click *Delete*. The product is deleted.

c. Click *Add*. The *Address Properties* dialog box displays with the *IP Address* page open.

d. Type a product description in the *Description* field.

e. Type the product IP address (determined by the network administrator) in the *IP Address* field.

f. Type the product subnet mask (determined by the network administrator) in the *Subnet Mask* field.

g. Click the *Product Type and Access* tab. Select *Switch* from the *Product Type* drop-down list and type customer-specified values in the *User ID*, *Password*, and *Retype Password* fields.

h. Click *OK* to close the dialog box and define the new product configuration to the SAN management application.

i. Click *OK* to close the *Discover Setup* dialog box.

Was the maintenance action successful?

NO **YES**

↓ The management server connection is restored. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

MAP 0400: Part failure analysis

This MAP describes fault isolation for product parts.

NOTE: The event log will indicate a FRU, regardless of whether the part is actually a customer-replaceable unit or a field-replaceable unit.

One or more of the following indicate a failure:

- Illumination of the associated amber LED.
- Event code **300**, **301**, **302**, **303**, **304**, **305**, **370**, **426**, **433**, **440**, **810**, **811**, **812**, or **850** observed at the *Event Log* (EFCM Basic Edition or Element Manager interface).

1

Table 12 lists event codes, explanations, and MAP steps.

Table 12 MAP 400 event codes

Event code	Explanation	Action
300	Cooling fan propeller failed.	Go to step 2.
301	Cooling fan propeller failed.	Go to step 2.
302	Cooling fan propeller failed.	Go to step 2.
303	Cooling fan propeller failed.	Go to step 2.
304	Cooling fan propeller failed.	Go to step 2.
305	Cooling fan propeller failed.	Go to step 2.
370	Cooling fan status polling temporarily disabled.	Go to step 3.
426	Multiple ECC single-bit errors occurred.	Go to step 4.
433	Non-recoverable Ethernet fault.	Go to step 5.
440	Embedded port hardware failed.	Go to step 5.
810	High temperature warning (CTP thermal sensor).	Go to step 6.
811	Critically hot temperature warning (CTP thermal sensor).	Go to step 6.
812	CTP card shutdown due to thermal violations.	Go to step 6.
850	Switch shutdown due to CTP thermal violations.	Go to step 6.

2

Visual inspection (amber LED illuminated) or event code **300**, **301**, **302**, **303**, **304**, or **305** indicates one or more cooling fans failed, and one or both power supplies must be removed and replaced. Refer to *Field-replaceable unit: Redundant power supply*.

- The procedure is concurrent and performed while the product is operational.
- If multiple fan failures caused a thermal shutdown, connect the product to facility AC power after power supply(s) are replaced.

- Perform a data collection as part of the removal and replacement. Refer to *Collect maintenance data* (EFCM Basic Edition) or *Collect maintenance data* (Element Manager).

NOTE: Do not remove a power supply unless a replacement part is available. To avoid product overheating, a removed power supply must be replaced within five minutes.

Was the maintenance action successful?

NO **YES**

↓ The product is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

3

As indicated by event code **370**, cooling fan status polling is temporarily disabled and status values for one or more fans exceed a set threshold. This indicates possible fan degradation or failure.

Is this event code a recurring problem?

NO **YES**

↓ A fan failure is indicated. **Go to step 2.**

Monitor fan operation or recording of additional failure event codes. **Exit MAP.**

4

As indicated by event code **426**, an intermittent synchronous dynamic random access memory (SDRAM) problem may result in switch failure.

Is this event code a recurring problem?

NO **YES**

↓ A CTP card failure is indicated. Replace the switch. **Exit MAP.**

Perform a data collection and contact the next level of support. Refer to *Collect maintenance data* (EFCM Basic Edition) or *Collect maintenance data* (Element Manager). **Exit MAP.**

5

As indicated by event code **433** or **440**, the CTP card failed. Replace the switch. **Exit MAP.**

6

As indicated by event code **810**, **811**, **812**, or **850**, an intermittent thermal problem may result in switch failure. Reset the product. Refer to *IML or reset switch* for instructions.

Was the maintenance action successful?

NO **YES**

↓ The product is operational. **Exit MAP.**

A CTP card failure is indicated. Replace the switch. **Exit MAP.**

MAP 0500: Port failure or link incident analysis

This MAP describes fault isolation for small form factor pluggable (SFP) optical transceivers and Fibre Channel link incidents. One or more of the following indicate a failure:

- Event code **080**, **081**, **083**, **506**, **507**, **512**, **514**, **515**, or **516** observed at the *Event Log* (EFCM Basic Edition or Element Manager interface).
- Event code **581**, **582**, **583**, **584**, **585**, or **586** observed at the console of an OSI server attached to the product reporting the problem.
- An error message observed at the *Link Incident Log* (EFCM Basic Edition or Element Manager interface).

1

Table 13 lists event codes, explanations, and MAP steps.

Table 13 MAP 500 event codes

Event code	Explanation	Action
080	Unauthorized worldwide name.	Go to step 2.
081	Invalid attachment.	Go to step 3.
083	Port set to inactive state.	Go to step 13.

Table 13 MAP 500 event codes (Continued)

Event code	Explanation	Action
506	Fibre Channel port failure.	Go to step 17.
507	Loopback diagnostics port failure.	Go to step 18.
512	Optical transceiver nonfatal error.	Go to step 17.
514	Optical transceiver failure.	Go to step 17.
515	Optical digital diagnostics warning threshold exceeded.	Go to step 17.
516	Optical digital diagnostics alarm threshold exceeded.	Go to step 17.
581	Implicit incident.	Go to step 19.
582	Bit error threshold exceeded.	Go to step 19.
583	Loss of signal or loss of synchronization.	Go to step 19.
584	Not operational primitive sequence received.	Go to step 19.
585	Primitive sequence timeout.	Go to step 19.
586	Invalid primitive sequence received for current link state.	Go to step 19.

Table 14 lists link incident messages and MAP steps.

Table 14 Link incident messages

Explanation	Action
Link interface incident - implicit incident.	Go to step 19.
Link interface incident - bit-error threshold exceeded.	Go to step 19.
Link failure - loss of signal or loss of synchronization.	Go to step 19.
Link failure - not-operational primitive sequence (NOS) received.	Go to step 19.
Link failure - primitive sequence timeout.	Go to step 19.
Link failure - invalid primitive sequence received for current link state.	Go to step 19.

2

As indicated by event code **080**, the eight-byte (16-digit) worldwide name (WWN) is not valid or an unconfigured nickname was used.

a. For the product reporting the problem:

   — **EFCM Basic Edition -** Select *Node List* from the *Product* menu at any view. The *Node List View* displays.

   — **Element Manager -** Select the *Node List* tab at any view. The *Node List View* displays.

b. At the *Port WWN* column, inspect the WWN assigned to the port or attached device.

c. The WWN must be entered in (***XX:XX:XX:XX:XX:XX:XX:XX***) format or must be a valid nickname. Ensure a valid WWN or nickname is entered.

Was the maintenance action successful?

NO **YES**

↓ The product port is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

3

As indicated by event code **081**, a port has an invalid attachment.

a. At the *Event Log*, examine the first five bytes of event data.

b. Byte **0** specifies the port reporting the problem. Byte **4** specifies the invalid attachment reason as listed in Table 15.

Table 15 Invalid attachment reasons and actions

Byte 4	Invalid attachment reason	Action
01	Unknown	Contact the next level of support.
02	ISL connection not allowed.	Go to step 4.
03, 04	Incompatible switch.	Go to step 5.
05	Loopback plug connected.	Go to step 6.
06	N-Port connection not allowed.	Go to step 4.
07	Non-IBM switch at other end.	Go to step 5.

Table 15 Invalid attachment reasons and actions (Continued)

Byte 4	Invalid attachment reason	Action
08	E_Port capability disabled.	Go to step 7.
0A	Unauthorized port binding WWN.	Go to step 2.
0B	Unresponsive node.	Go to step 8.
0C	ESA security mismatch.	Go to step 10.
0D	Fabric binding mismatch.	Go to step 11.
0E	Authorization failure reject.	Go to step 8.
0F	Unauthorized switch binding WWN.	Go to step 10.
10	Authentication failure	Go to step 12.
11	Fabric mode mismatch.	Go to step 5.

4

A connection is not allowed because of a conflict with the configured port type. An expansion port (E_Port) is cabled to a Fibre Channel device or a fabric port (F_Port) is cabled to a director or switch.

a. For the product reporting the problem:
   - — **EFCM Basic Edition -** Select *Ports* and *Basic Info* from the *Configure* menu at any view. The *Basic Information View* displays.
   - — **Element Manager -** Select *Ports* from the *Configure* menu at any view. The *Configure Ports* dialog box displays.

b. If necessary, use the vertical scroll bar to display the information row for the port indicating an invalid attachment.

c. Select (click) the *Type* field and configure the port as follows:
   - Select fabric port (**F_Port**) if the port is cabled to a device.
   - Select expansion port (**E_Port**) if the port is cabled to a director or switch (ISL).

d. Click *OK* or *Activate*.

Was the maintenance action successful?

NO **YES**

↓ The product port is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

5

An ISL connection is not allowed because one of the following mode-mismatch conditions was detected:

- The product is configured to operate in **Open Fabric 1.0** mode and is connected to a fabric element not configured to **Open Fabric 1.0** mode.
- The product is configured to operate in **Open Fabric 1.0** mode and is connected to a legacy IBM switch at the incorrect exchange link parameter (ELP) revision level.
- The product is configured to operate in **Open Fabric 1.0** mode and is connected to a non-IBM switch at the incorrect ELP revision level.
- The product is configured to operate in **McDATA Fabric 1.0** mode and is connected to a non-IBM switch.

Reconfigure the operating mode:

a. Set the product offline. Refer to *Set online state* (EFCM Basic Edition) or *Set online state* (Element Manager).

b. For the product reporting the problem:

   — **EFCM Basic Edition -** Select *Switch* and *Fabric Parameters* from the *Configure* menu at any view. The *Fabric Parameters View* displays.

   — **Element Manager -** Select *Operating Parameters* and *Fabric Parameters* from the *Configure* menu at any view. The *Configure Fabric Parameters* dialog box displays.

c. Select **McDATA Fabric 1.0** or **Open Fabric 1.0** from the *Interop Mode* drop-down list.

   — Select **McDATA Fabric 1.0** if the product is attached *only* to other IBM directors or switches operating in **McDATA Fabric 1.0** mode.

— Select **Open Fabric 1.0** if the product is attached to directors or switches produced by open-fabric compliant original equipment manufacturers (OEMs).

d. Click *OK* or *Activate*.

Was the maintenance action successful?

NO **YES**

↓ The product port is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

6

A loopback (wrap) plug is connected to the port with no diagnostic running. Remove the plug from the port receptacle. If directed by the customer, connect a fiber-optic jumper cable attaching a device to the product.

- If the port is operational with no device attached, both LEDs adjacent to the port extinguish and the port state is *No Light*.
- If the port is operational with a device attached, the green LED illuminates, the amber LED extinguishes, and the port state is *Online*.

Was the maintenance action successful?

NO **YES**

↓ The product port is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

7

An ISL connection is not allowed because E_Port capability is disabled. Install the full-fabric PFE key to enable E_port capability. Refer to *Install PFE keys (optional)* (EFCM Basic Edition) or *Task 15: Configure PFE key (optional)* (Element Manager). **Exit MAP.**

8

The connection timed out because of an unresponsive device or an ISL security violation (authorization failure reject). Check port status and clean fiber-optic components.

a. Inform the customer the port will be blocked. Ensure the system administrator quiesces Fibre Channel frame traffic and sets attached devices offline.

b. Block the port. Refer to *Block or unblock a port* (EFCM Basic Edition) or *Block or unblock a port* (Element Manager).

c. Clean fiber-optic connectors. Refer to *Clean fiber-optic components*.

d. Unblock the port. Refer to *Block or unblock a port* (EFCM Basic Edition) or *Block or unblock a port* (Element Manager).

e. Monitor port operation for approximately five minutes.

Was the maintenance action successful?

NO **YES**

↓ The product port is operational. **Exit MAP.**

9

Inspect and service host bus adapters (HBAs).

Was the maintenance action successful?

NO **YES**

↓ The product port is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

10

A connection is not allowed because of a switch binding or exchange security attribute (ESA) feature mismatch. Switch binding parameters must be compatible for both fabric elements. At the EFCM Basic Edition interface or Element Manager, ensure switch binding is enabled, the connection policy is compatible, and switch membership lists are compatible for both elements.

- **EFCM Basic Edition -** Refer to the *EFCM Basic Edition User Manual* (620-000240) for instructions.
- **Element Manager -** Refer to the *Element Manager User Manual* (620-000242) for instructions.

Was the maintenance action successful?

NO **YES**

↓ The product port is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

11

A connection is not allowed because of a fabric binding mismatch. Fabric membership lists must be compatible for both elements. At the

EFCM Basic Edition interface or SAN management application, ensure fabric binding is enabled and fabric membership lists are compatible for both elements.

- **EFCM Basic Edition -** Refer to the *EFCM Basic Edition User Manual* (620-000240) for instructions.
- **SAN management application -** Refer to the *SANavigator Software Release 4.2 User Manual* (621-000013) or *EFC Manager Software Release 8.7 User Manual* (620-000170) for instructions.

Was the maintenance action successful?

NO **YES**

↓ The product port is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

12

A connection is not allowed because of a SANtegrity authentication failure. At the EFCM Basic Edition interface or Element Manager, modify the IP address access control list, product-level authentication settings, port-level authentication settings, and challenge handshake authentication protocol (CHAP) sequence to ensure device access to the product.

- **EFCM Basic Edition -** Refer to the *EFCM Basic Edition User Manual* (620-000240) for instructions.
- **Element Manager -** Refer to the *Element Manager User Manual* (620-000242) for instructions.

Was the maintenance action successful?

NO **YES**

↓ The product port is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

13

As indicated by event code **083**, a port is set to an inactive state.

a. At the *Event Log*, examine the first two bytes of event data.

b. Byte **0** specifies the port reporting the problem. Byte **1** specifies the inactive reason as listed in Table 16.

Table 16 Inactive port reasons and actions

Byte 1	Inactive port reason	Action
02	Feature key not enabled.	Go to step 14.
03	Switch speed conflict.	Go to step 15.
04	Optics speed conflict.	Go to step 15.
06	Port swap conflict.	Go to step 16.

14

A port is inactive because Flexport Technology is disabled. Install the Flexport Technology PFE key to enable N_Port capability. Refer to *Install PFE keys (optional)* (EFCM Basic Edition) or *Task 15: Configure PFE key (optional)* (Element Manager). **Exit MAP.**

15

A port is inactive because the:

- Port cannot operate at the product (backplane) speed.
- Optical transceiver does not support the configured port speed.

Change the port speed to be compatible with the backplane or optical transceiver speed.

a. For the product reporting the problem:

   — **EFCM Basic Edition -** Select *Ports* and *Basic Info* from the *Configure* menu at any view. The *Basic Information View* displays.

   — **Element Manager -** Select *Ports* from the *Configure* menu at any view. The *Configure Ports* dialog box displays.

b. If necessary, use the vertical scroll bar to display the information row for the inactive port.

c. Select (click) the *Speed* field and configure the port.

d. Click *OK* or *Activate*.

Was the maintenance action successful?

NO **YES**

↓ The product port is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

16

A port is inactive because the port swap configuration is invalid. Perform a port swap procedure (Element Manager only), ensure the configuration is valid, and ensure the port address matches the hardware configuration definition (HCD) of the attached host. Refer to *Swap ports*. **Exit MAP.**

17

As indicated by event codes **506**, **512**, **514**, **515**, or **516**, a port failed and the optical transceiver must be removed and replaced. Refer to *Customer-replaceable unit: SFP optical transceiver*.

- The procedure is concurrent and performed while the product is operational.
- Replace the transceiver with a transceiver of the same type (shortwave or longwave) and speed.
- Perform an external loopback test. Refer to *External loopback test* (EFCM Basic Edition) or *External loopback test* (Element Manager).

NOTE: Event code **514** may generate a call-home event that incorrectly indicates a CTP card failure. Although the optical socket on the CTP card may have failed, replace the transceiver and verify operation. If a failure is still indicated, replace the switch. When event code **514** is indicated, ensure a replacement transceiver and switch are available.

Was the maintenance action successful?

NO **YES**

↓ The product port is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

18

As indicated by event code **507**, a port failed a loopback test. Reset the failed port.

a. At the EFCM Basic Edition interface:

   1. Select *Ports* and *Reset* from the *Maintenance* menu at any view. The *Reset View* displays.
   2. If necessary, use the vertical scroll bar to display the information row for the port.
   3. Select (click) the check box in the *Reset* column.
   4. Click *OK*. The port resets.

b. At the Element Manager:

   1. At the *Hardware View*, right-click the port. A pop-up menu appears.
   2. Select *Reset Port*. The message **This operation will cause a link reset to be sent to the attached device** displays.
   3. Click *OK*. The port resets.

c. Perform an external loopback test for the reset port. Refer to *External loopback test* (EFCM Basic Edition) or *External loopback test* (Element Manager).

Was the maintenance action successful?

NO **YES**

↓ The product port is operational. **Exit MAP.**

Go to step 17.

19

A message appeared in the *Link Incident Log* or an event code **581**, **582**, **583**, **584**, **585**, or **586** was observed at the console of an OSI server attached to the product reporting the problem. Clear the link incident (Element Manager only).

a. At the *Hardware View*, right-click the port. A pop-up menu appears.

b. Select *Clear Link Incident Alert(s)*. The *Clear Link Incident Alert(s)* dialog box displays.

c. Select the *This port (**n**) only* radio button and click *OK*. The link incident clears.

d. Monitor port operation for approximately five minutes.

Did the link incident recur?

YES **NO**

↓ The problem is transient and the product port is operational. **Exit MAP.**

20

Clean fiber-optic components.

a. Inform the customer the port will be blocked. Ensure the system administrator quiesces Fibre Channel frame traffic and sets attached devices offline.

b. Block the port. Refer to *Block or unblock a port* (EFCM Basic Edition) or *Block or unblock a port* (Element Manager).

c. Clean fiber-optic connectors. Refer to *Clean fiber-optic components*.

d. Unblock the port. Refer to *Block or unblock a port* (EFCM Basic Edition) or *Block or unblock a port* (Element Manager).

e. Monitor port operation for approximately five minutes.

Did the link incident recur?

YES **NO**

↓ The product port is operational. **Exit MAP.**

21

Disconnect the fiber-optic jumper cable from the port and connect the cable to a spare port.

Is a link incident reported at the new port?

YES **NO**

↓ The port reporting the problem is causing the link incident. This indicates port degradation and a possible pending failure. **Go to step 17.**

22

Ensure the attached fiber-optic jumper cable is not bent and connectors are not damaged. If the cable is bent or connectors are damaged:

a. Inform the customer the port will be blocked. Ensure the system administrator quiesces Fibre Channel frame traffic and sets attached devices offline.

b. Block the port. Refer to *Block or unblock a port* (EFCM Basic Edition) or *Block or unblock a port* (Element Manager).

c. Remove and replace the fiber-optic jumper cable.

d. Unblock the port. Refer to *Block or unblock a port* (EFCM Basic Edition) or *Block or unblock a port* (Element Manager).

Was the maintenance action successful?

NO **YES**

↓ The product port is operational. **Exit MAP.**

23

The attached device is causing the recurrent link incident. Inform the customer of the problem and have the system administrator:

a. Inspect and verify operation of the attached device.

b. Repair the attached device if a failure is indicated.

c. Monitor port operation for approximately five minutes.

Was the maintenance action successful?

NO **YES**

↓ The product port is operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

MAP 0600: Fabric or ISL problem analysis

This MAP describes fault isolation for fabric, interswitch link (ISL), fenced E_Port, and segmented E_Port problems. The failure indicator is an event code **011**, **021**, **051**, **061**, **062**, **063**, **070**, **071**, **072**, **082**, **140**, **142**, or **150** observed at the *Event Log* (EFCM Basic Edition or Element Manager interface).

1

Table 17 lists event codes, explanations, and MAP steps.

Table 17 MAP 600 event codes

Event code	Explanation	Action
011	Login Server database invalid.	Go to step 2.
021	Name Server database invalid.	Go to step 2.
051	Management Server database invalid.	Go to step 3.
061	Fabric Controller database invalid.	Go to step 4.
062	Maximum interswitch hop count exceeded.	Go to step 5.
063	Remote switch has too many ISLs.	Go to step 6.
070	E_Port is segmented.	Go to step 7.
071	Switch is isolated.	Go to step 7.
072	E_Port connected to unsupported switch.	Go to step 15.
082	Port fenced.	Go to step 16.
140	Congestion detected on an ISL.	Go to step 21.
142	Low BB_Credit detected on an ISL.	Go to step 21.
150	Fabric merge failure.	Go to step 22.

2

A minor error occurred that caused the Fabric Services database to be re-initialized to an empty state, and a disruptive fabric logout and login occurred for all attached devices. Indications are:

- **Event code 011 -** The Login Server database failed cyclic redundancy check (CRC) validation.
- **Event code 021 -** The Name Server database failed CRC validation.

Devices resume operation after fabric login. Perform a data collection and contact the next level of support. Refer to *Collect maintenance data* (EFCM Basic Edition) or *Collect maintenance data* (Element Manager). **Exit MAP.**

3

As indicated by event code **051**, a minor error occurred that caused the Management Server database to be re-initialized to an empty state and fail CRC validation. A disruptive server logout and login occurred for all attached devices.

Devices resume operation after Management Server login. Perform a data collection and contact the next level of support. Refer to *Collect maintenance data* (EFCM Basic Edition) or *Collect maintenance data* (Element Manager). **Exit MAP.**

4

As indicated by event code **061**, a minor error occurred that caused the Fabric Controller database to be re-initialized to an empty state and fail CRC validation. The product briefly lost interswitch link capability.

Interswitch links resume operation after CTP reset. Perform a data collection and contact the next level of support. Refer to *Collect maintenance data* (EFCM Basic Edition) or *Collect maintenance data* (Element Manager). **Exit MAP.**

5

As indicated by event code **062**, Fabric Controller software detected a path to another fabric element (director or switch) that traverses more than three interswitch links (hops). Fibre Channel frames may persist in the fabric longer than timeout values allow.

Advise the customer of the problem and reconfigure the fabric so the path between any two fabric elements does not traverse more than three hops.

Was the maintenance action successful?

NO **YES**

↓ The fabric, ISL, and product are operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

6

As indicated by event code **063**, Fabric Controller software detected:

- A fabric element with more than 32 ISLs (SAN management application Version 3.2 or earlier).
- A fabric element with more than 128 ISLs (SAN management application Version 3.3 or later).

Fibre Channel frames may be lost or directed in loops because of potential fabric routing problems. Advise the customer of the problem and reconfigure the fabric so that no directors or switches have more than the proscribed number of ISLs.

Was the maintenance action successful?

NO **YES**

↓ The fabric, ISL, and product are operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

7

Event code **070** indicates an E_Port detected an incompatibility with an attached fabric element, segmented the port, and prevented fabric participation. A segmented E_port cannot transmit Class 2 or Class 3 Fibre Channel traffic. Event code **071** indicates the product is isolated from all fabric elements, and is accompanied by an event code **070** for each segmented E_Port. Event code **071** is resolved when all **070** events are corrected. Obtain supplementary event data as follows:

a. At the *Event Log*, examine the first five bytes of event data.

b. Byte **0** specifies the segmented E_port. Byte **4** specifies the segmentation reason as listed in Table 18. The reason also displays at the *Port List View* (EFCM Basic Edition) or *Port Properties* dialog box (Element Manager).

Table 18 E_Port segmentation reasons and actions

Byte 4	Segmentation reason	Action
01	Incompatible operating parameters.	Go to step 8.
02	Duplicate domain ID.	Go to step 9.
03	Incompatible zoning configurations.	Go to step 10.
04	Build fabric protocol error.	Go to step 11.
05	No principal switch.	Go to step 13.
06	No response from attached switch (hello timeout).	Go to step 14.

8

An E_Port segmented because the error detect time out value (E_D_TOV) or resource allocation time out value (R_A_TOV) is incompatible with the attached fabric element.

a. Contact customer support or engineering personnel to determine the recommended E_D_TOV and R_A_TOV values for both fabric elements.

b. Inform the customer both products will be set offline. Ensure the system administrator quiesces Fibre Channel frame traffic and sets attached devices offline.

c. Set both products offline. Refer to *Set online state* (EFCM Basic Edition) or *Set online state* (Element Manager).

d. For the first product reporting the problem:

   — **EFCM Basic Edition -** Select *Switch* and *Fabric Parameters* from the *Configure* menu at any view. The *Fabric Parameters View* displays.

   — **Element Manager -** Select *Operating Parameters* and *Fabric Parameters* from the *Configure* menu at any view. The *Configure Fabric Parameters* dialog box displays.

e. Type the recommended E_D_TOV and R_A_TOV values, then click *OK* or *Activate*.

f. Repeat steps **d** and **e** at the second product (attached to the segmented E_Port). Use the same E_D_TOV and R_A_TOV values.

g. Set both products online. Refer to *Set online state* (EFCM Basic Edition) or *Set online state* (Element Manager).

Was the maintenance action successful?

NO **YES**

↓ The fabric, ISL, and product are operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

9

An E_Port segmented because two fabric elements had duplicate domain IDs.

a. Determine the desired domain ID (**1** through **31** inclusive) for each product.

b. Inform the customer both products will be set offline. Ensure the system administrator quiesces Fibre Channel frame traffic and sets attached devices offline.

c. Set both products offline. Refer to *Set online state* (EFCM Basic Edition) or *Set online state* (Element Manager).

d. For the first product reporting the problem:

   — **EFCM Basic Edition -** Select *Switch* and *Parameters* from the *Configure* menu at any view. The *Parameters View* displays.

   — **Element Manager -** Select *Switch Parameters* and *Fabric Parameters* from the *Configure* menu at any view. The *Configure Switch Parameters* dialog box displays.

e. Type the customer-determined preferred domain ID value, then click *OK* or *Activate*.

f. Repeat steps **d** and **e** at the second product (attached to the segmented E_Port). Use a different preferred domain ID value.

g. Set both products online. Refer to *Set online state* (EFCM Basic Edition) or *Set online state* (Element Manager).

Was the maintenance action successful?

NO **YES**

↓ The fabric, ISL, and product are operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

10

An E_Port segmented because two products had incompatible zoning configurations. An identical zone name is recognized in the active zone set for both products, but the zones contain different members.

a. Determine the desired zone name change for one of the affected products. Zone names must conform to the following rules:

   — The name must be 64 characters or fewer in length.

   — The first character must be a letter (**a** through **z**), upper or lower case.

   — Other characters must be alphanumeric (**a** through **z** or **0** through **9**), dollar sign (**$**), hyphen (**-**), caret (**^**), or underscore (_).

b. At the EFCM Basic Edition interface or SAN management application, inspect names in the active zone set to determine the incompatible zone name, then modify the name as directed by the customer:

   — **EFCM Basic Edition -** Refer to the *EFCM Basic Edition User Manual* (620-000240) for instructions.

   — **SAN management application -** Refer to the *SANavigator Software Release 4.2 User Manual* (621-000013) or *EFC Manager Software Release 8.7 User Manual* (620-000170) for instructions.

Was the maintenance action successful?

NO **YES**

↓ The fabric, ISL, and product are operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

11

An E_Port segmented because a build fabric protocol error was detected.

a. Disconnect the fiber-optic jumper cable from the segmented E_Port.

b. Reconnect the cable to the same port.

Was the maintenance action successful?

NO **YES**

↓ The fabric, ISL, and product are operational. **Exit MAP.**

12

Reset the product. Refer to *IML or reset switch* for instructions.

Was the maintenance action successful?

NO **YES**

↓ The fabric, ISL, and product are operational. **Exit MAP.**

Perform a data collection and contact the next level of support. Refer to *Collect maintenance data* (EFCM Basic Edition) or *Collect maintenance data* (Element Manager). **Exit MAP.**

13

An E_Port segmented because no product in the fabric is capable of becoming the principal switch.

a. Inform the customer the product will be set offline. Ensure the system administrator quiesces Fibre Channel frame traffic and sets attached devices offline.

b. Set the product offline. Refer to *Set online state* (EFCM Basic Edition) or *Set online state* (Element Manager).

c. For the product reporting the problem:

   — **EFCM Basic Edition -** Select *Switch* and *Fabric Parameters* from the *Configure* menu at any view. The *Fabric Parameters View* displays.

   — **Element Manager -** Select *Operating Parameters* and *Fabric Parameters* from the *Configure* menu at any view. The *Configure Fabric Parameters* dialog box displays.

d. At the *Switch Priority* field, select *Principal*, *Never Principal*, or *Default*, then click *OK* or *Activate*. The switch priority value designates the fabric's principal switch, which is assigned a priority of **1** and controls the allocation and distribution of domain IDs for all fabric elements (including itself).

   Principal is the highest priority setting, *Default* is the next highest, and *Never Principal* is the lowest priority setting. The setting *Never Principal* means the fabric element is incapable of becoming a principal switch. If all elements are set to *Principal* or *Default*, the element with the highest priority and the lowest WWN becomes the principal switch. At least one element in a multiswitch fabric must be set as *Principal* or *Default*. If all elements are set to *Never Principal*, all ISLs segment.

e. Set the product online. Refer to *Set online state* (EFCM Basic Edition) or *Set online state* (Element Manager).

Was the maintenance action successful?

NO **YES**

↓ The fabric, ISL, and product are operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

14

An E_Port segmented (operational product) because a response (hello timeout) to a verification check indicates an attached switch is not operational.

a. Perform a data collection at the operational product and contact the next level of support. Refer to *Collect maintenance data* (EFCM Basic Edition) or *Collect maintenance data* (Element Manager).

b. Go to *MAP 0000: Start MAP* and perform fault isolation for the failed switch. **Exit MAP.**

15

Event code **072** indicates a product E_Port is connected to an unsupported fabric element. Advise the customer of the problem and disconnect the ISL to the unsupported fabric element. **Exit MAP.**

16

Event code **082** is informational only and indicates a product E_Port is fenced (blocked). An application or hardware malfunction occurred (as indicated by failure symptoms or primary event codes) or the port fencing policy is too restrictive. Obtain supplementary event data as follows:

a. At the *Event Log*, examine the first five bytes (**0** through **4**) of event data.

b. Byte **0** specifies the E_Port reporting the problem. Byte **4** specifies the port fence code as listed in Table 19.

Table 19 Port fence codes and actions

Byte 4	Port fence code	Action
01	Protocol error.	Go to step 17.
02	Link-level hot I/O.	Go to step 18.
03	Security violation.	Go to step 19.

17

An E_Port is fenced because of a protocol error. Depending on failure cause, additional information and event codes are available at the product or attached switch. Perform one of the following:

- The E_Port is segmented and accompanied by primary event code **070**. **Go to step 7.**
- The fiber-optic cable is disconnected, the cable failed or is degraded, or the port optical transceiver failed. The failure is accompanied by a primary event code indicating the failure type. Go to *MAP 0000: Start MAP* and perform fault isolation for the primary event code. **Exit MAP.**
- The E_Port is fenced because of persistent incomplete operations (ISL bouncing). Go to *MAP 0000: Start MAP* and perform fault isolation at the attached switch. **Exit MAP.**
- The E_Port is fenced because of application-layer protocol errors. Go to *MAP 0000: Start MAP* and perform fault isolation at the attached switch. **Exit MAP.**

18

An E_Port is fenced because devices connected to the attached fabric element are flooding the ISL with frames (hot I/O). These link-level problems are typically associated with legacy devices, arbitrated loop devices, or magnetic tape drives. Perform one of the following:

- Disconnect the ISL. **Exit MAP.**
- Refer to the manufacturer's documentation and perform fault isolation at the attached device or fabric element. **Exit MAP.**
- Change port fencing threshold settings to more lenient values. **Go to step 20.**

19

An E_Port is fenced because of persistent firmware-related security violations (SANtegrity binding or SANtegrity authentication failures).

a. At the EFCM Basic Edition interface, SAN management application, or Element Manager, change binding membership lists or authentication parameters as directed by the customer:

   — **EFCM Basic Edition -** Refer to the *EFCM Basic Edition User Manual* (620-000240) for instructions.

— **SAN management application -** Refer to the *SANavigator Software Release 4.2 User Manual* (621-000013) or *EFC Manager Software Release 8.7 User Manual* (620-000170) for instructions.

— **Element Manager -** Refer to the *Element Manager User Manual* (620-000242) for instructions.

b. Unblock the port. Refer to *Block or unblock a port* (EFCM Basic Edition) or *Block or unblock a port* (Element Manager).

Was the maintenance action successful?

NO **YES**

↓ The fabric, ISL, and product are operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

20

Port fencing threshold settings are too restrictive.

a. At the EFCM Basic Edition interface or SAN management application, change port fencing threshold settings to more lenient values as directed by the customer:

— **EFCM Basic Edition -** Refer to the *EFCM Basic Edition User Manual* (620-000240) for instructions.

— **SAN management application -** Refer to the *SANavigator Software Release 4.2 User Manual* (621-000013) or *EFC Manager Software Release 8.7 User Manual* (620-000170) for instructions.

b. Unblock the port. Refer to *Block or unblock a port* (EFCM Basic Edition) or *Block or unblock a port* (Element Manager).

Was the maintenance action successful?

NO **YES**

↓ The fabric, ISL, and product are operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

21

Event codes **140** and **142** occur only if the optional OpenTrunking feature is enabled.

- **Event code 140 -** OpenTrunking firmware detected an ISL with Fibre Channel traffic that exceeds the configured congestion threshold.
- **Event code 142 -** OpenTrunking firmware detected an ISL with no transmission BB_Credit for a period of time that exceeded the configured low BB_Credit threshold. This results in downstream fabric congestion.

No action is required for an isolated event or if the reporting ISL approaches 100% throughput. If the event persists, perform one of the following:

- Relieve the congestion by adding parallel ISLs between the fabric elements reporting the problem.
- Increase the ISL link speed between the fabric elements reporting the problem (from 1 Gbps to 2 or 4 Gbps).
- Reroute Fibre Channel traffic by moving device connections to a less-congested region of the fabric.

Was the maintenance action successful?

NO **YES**

↓ The fabric, ISL, and product are operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

22

Event code **150** indicates a fabric merge process failed during ISL initialization. An incompatible zone set was detected or a problem occurred during delivery of a zone merge frame. This event code always precedes event code **070**, and represents the reply of an adjacent fabric element in response to a zone merge frame. Obtain supplementary event data as follows:

a. At the *Event Log*, examine the first 12 bytes (**0** through **11**) of event data.

b. Bytes **0** specifies the E_Port reporting the problem. Bytes **8** through **11** specify the failure reason as listed in Table 20.

Table 20 Fabric merge failure reasons and actions

Bytes 8 - 11	Merge failure reason	Action
01	Invalid data length.	Go to step 23.
08	Invalid zone set format.	Go to step 23.
09	Invalid data.	Go to step 24.
0A	Cannot merge.	Go to step 24.
F0	Retry limit reached.	Go to step 23.
F1	Invalid response length.	Go to step 23.
F2	Invalid response code.	Go to step 23.

23

A zone merge process failed during ISL initialization. The following list explains the reason:

- **Reason 01 -** An invalid data length condition caused an error in a zone merge frame.
- **Reason 08 -** An invalid zone set format caused an error in a zone merge frame.
- **Reason F0 -** A retry limit reached condition caused an error in a zone merge frame.
- **Reason F1 -** An invalid response length condition caused an error in a zone merge frame.
- **Reason F2 -** An invalid response code caused an error in a zone merge frame.

Disconnect the fiber-optic jumper cable from the E_Port reporting the problem, then reconnect the cable to the same port.

Was the maintenance action successful?

NO **YES**

↓ The fabric, ISL, and product are operational. **Exit MAP.**

Perform a data collection and contact the next level of support. Refer to *Collect maintenance data* (EFCM Basic Edition) or *Collect maintenance data* (Element Manager). **Exit MAP.**

24

A zone merge process failed during ISL initialization. The following list explains the reason:

- **Reason 09 -** Invalid data caused a zone merge failure.
- **Reason 0A -** A *Cannot Merge* condition caused a zone merge failure.

Obtain supplementary error code data for event code **150**. At the *Event Log*, examine bytes **12** through **15** of event data that specify the error code. Record the error code.

Perform a data collection and contact the next level of support. Refer to *Collect maintenance data* (EFCM Basic Edition) or *Collect maintenance data* (Element Manager). Report the event code, associated failure reason, and supplementary error code. **Exit MAP.**

Chapter 4: Repair information

This chapter describes repair-related procedures for the switch. The procedures are performed at the switch, a browser-capable PC communicating with the product-resident Enterprise Fabric Connectivity Manager (EFCM) Basic Edition interface, or a rack-mount management server running a storage area network (SAN) management application. The chapter describes:

- *Procedural notes* on page 153
- *Power on switch* on page 153
- *Power off switch* on page 155
- *IML or reset switch* on page 155
- *Clean fiber-optic components* on page 157
- *Download firmware* on page 158
- *Port LED diagnostics* on page 159
- *Repair procedures - EFCM Basic Edition* on page 160
- *Repair procedures - SAN management application* on page 181

Procedural notes

Note the following:

1. Follow all electrostatic discharge (ESD) precautions and **DANGER**, **CAUTION**, and **ATTENTION** statements.
2. Read the procedure thoroughly to familiarize yourself with the information, before performing a procedure.

Power on switch

To power on the switch use the following steps:

1. Ensure that the correct power cords are available. One alternating current (AC) power cord is required for each power supply.

© Copyright IBM Corp. 2006

DANGER

Overloading a branch circuit is potentially a fire hazard and a shock hazard under certain conditions. To avoid these hazards, ensure that your system electrical requirements do not exceed branch circuit protection requirements. Refer to the information that is provided with your device or the power rating label for electrical specifications.
(D002)

2. Plug power cords into facility power sources and AC connectors at the rear of the switch. When the first power cord is connected, the switch powers on and performs power-on self-tests (POSTs).

   NOTE: For high availability, plug the power cords into separate facility power circuits.

   During POSTs:

   — The green **PWR** LED on the switch front panel illuminates.

   — The amber **ERR** LED on the switch front panel blinks momentarily as the switch is tested.

   — The green LED associated with the Ethernet port blinks momentarily as the port is tested.

   — The blue/green and amber LEDs associated with Fibre Channel ports blink momentarily as the ports are tested.

   The **PWR** LED remains illuminated and all amber LEDs extinguish after successful POST completion.

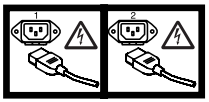
   If a POST error occurs, go to *MAP 0000: Start MAP* to isolate the problem.

Power off switch

Notify the customer that the switch is to be powered off. Ensure that the system administrator quiesces Fibre Channel frame traffic through the switch and sets attached devices offline.

To power off the switch:

1. Set the switch offline. Refer to *Set online state* (EFCM Basic Edition) or *Set online state* (SAN management application) for instructions.



DANGER

Multiple power cords (L003)

2. Disconnect power cords from the AC connectors at the rear of the switch.

IML or reset switch

ATTENTION! A reset should only be performed if a CTP card failure is indicated. Do not reset a switch unless directed to do so by a procedural step or the next level of support.

An initial machine load (IML) or reset is performed at the switch front panel using the **RESET** button. An IML does not cause power-on diagnostics to execute and is not disruptive to Fibre Channel traffic.

An IML:

- Reloads switch firmware from FLASH memory.
- Resets the Ethernet LAN interface, causing the connection to the browser PC or management server to drop momentarily until the connection automatically recovers.

A reset is disruptive to Fibre Channel traffic and resets the:

- Microprocessor and functional logic for the control processor (CTP) card and reloads the firmware from FLASH memory.

- Ethernet LAN interface, causing the connection to the browser PC or management server to drop momentarily until the connection automatically recovers.
- Ports, causing all Fibre Channel connections to drop momentarily until the connections automatically recover. This causes attached devices to log out and log back in, therefore data frames lost during switch reset must be retransmitted.

IML

To IML the switch use the following steps:

1. Press and hold the **RESET** button (about three seconds) until the amber **ERR** LED blinks at twice the unit beaconing rate.
2. Release the button. During the IML, the switch-to-browser PC (or management server) Ethernet link drops momentarily.

Reset

To reset the switch use the following steps:

1. Press and hold the **RESET** button for ten seconds.
   - — The amber **ERR** LED blinks at twice the unit beaconing rate on holding the button for three seconds.
   - — The **ERR** LED stops blinking, and all front panel LEDs illuminate on holding the button for ten seconds.
2. Release the button to reset the switch. During the reset:
   - — The green **PWR** LED on the switch front panel illuminates.
   - — The amber **ERR** LED on the switch front panel blinks momentarily while the switch is tested.
   - — The green LED associated with the Ethernet port blinks momentarily while the port is tested.
   - — Green and amber LEDs associated with Fibre Channel ports blink momentarily while the ports are tested.
   - — The switch-to-browser PC (or management server) Ethernet link drops momentarily.

Clean fiber-optic components

Perform this procedure as directed by a service procedural step or when connecting or disconnecting fiber-optic cables from port optical transceivers.

The following tools (supplied by service personnel) are required:

- ESD grounding cable and wrist strap.
- Fiber-optic cleaning kit with:
  - — Oil-free compressed air or HFC-134a aerosol duster.
  - — Alcohol-soaked cleaning pads.

CAUTION

Goggles are needed for the procedure.
(C011)

To clean fiber-optic components use the following steps:

1. Follow ESD procedures by attaching a wrist strap to the product chassis and your wrist.
2. Disconnect the fiber-optic cable from the optical transceiver as directed by a customer representative or service procedural step.
3. Use an aerosol duster to blow any contaminants from the component (part 1 of Figure 45).

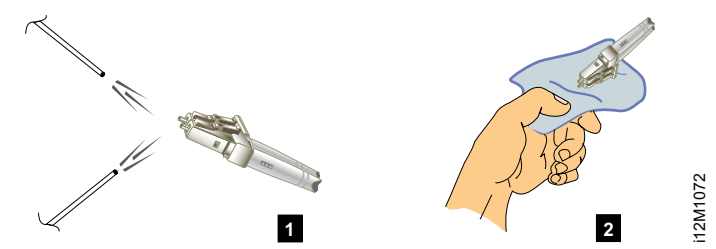


Figure 45 Clean fiber-optic components

  - — Hold the duster upright and keep the air nozzle approximately 50 millimeters (two inches) from the end of the component.

— Blow compressed air or HFC-134a gas on exposed surfaces and the end-face of the component for approximately five seconds.

4. Gently wipe the end-face and other surfaces of the component with an alcohol pad (part 2 of Figure 45). Ensure that the pad makes full contact with the surface to be cleaned. Wait approximately five seconds for cleaned surfaces to dry.
5. Repeat steps two and three (second cleaning).
6. Repeat steps two and three (third cleaning).
7. Reconnect the fiber-optic cable to the optical transceiver.

Download firmware

The firmware version shipped with the product is provided on the *System Version XX.YY.ZZ* CD-ROM. The SAN management application (software) shipped with the product is provided on the *EFC Management Applications* CD-ROM. Subsequent (upgrade) firmware and software versions are provided to customers through IBM.

NOTE: When upgrading firmware or software, follow all procedural information contained in release notes or engineering change (EC) instructions that accompany the version. Such information supplements information provided in this general procedure.

1. Obtain the latest level of firmware, at http://www.ibm.com/servers/storage/support/san/index.html. Locate the link for this switch and then select the link for downloading firmware.
2. Follow the instructions for downloading the firmware.
3. Transfer the downloaded firmware file to the rack-mount management server or PC communicating with the EFCM Basic Edition interface. Use a diskette, CD-ROM, or other electronic means.
4. Install the firmware as described in this guide.

Port LED diagnostics

Fibre Channel port diagnostic information is obtained by inspecting port LEDs at the product front panel or emulated port LEDs at the management interface (EFCM Basic Edition interface or SAN management application).

LEDs adjacent to each port and software alert symbols indicate operational status as described in Table 21.

Table 21 Port operational states

Port state	Green LED	Amber LED	Alert symbol	Description
Online	On or Blinking	Off	None	An attached device is ready to communicate, or is communicating with other devices. Green LED illuminates.
Offline	Off	Off	None	Port is blocked and transmitting the offline sequence (OLS) to attached device.
	Off	Off	Yellow Triangle	Port is unblocked and receiving the OLS, indicating attached device is offline.
Beaconing	Off, On, or Blinking	Blinking	Yellow Triangle	Port is beaconing. Amber LED blinks once every two seconds to enable users to locate port.
Invalid Attachment	On	Off	Yellow Triangle	Port has an invalid attachment. Reason appears as supplementary data in the *Event Log*.
Link Incident	Off	Off	Yellow Triangle	Link incident occurred. Reason appears in the *Link Incident Log*.
Link Reset	Off	Off	Yellow Triangle	Product and attached device are performing a link reset to recover the connection. Transient state that does not persist.
No Light	Off	Off	None	No signal (light) is received at product port. Normal condition when no cable is attached to port or when attached device is powered off.
Inactive	On	Off	Yellow Triangle	Port is inactive. Reason appears at *Port List View* or *Port Properties* dialog box.
Not Installed	Off	Off	None	Optical transceiver not installed in the port.
Not Operational	Off	Off	Yellow Triangle	Port is receiving the not operational sequence (NOS) from attached device.

Table 21 **Port operational states (Continued)**

Port state	Green LED	Amber LED	Alert symbol	Description
Port Failure	Off	On	Red and Yellow Blinking Diamond	Port failed and requires service.
Segmented E_Port	On	Off	Yellow Triangle	E_Port segmented, preventing connected switches from forming a fabric. Reason appears as supplementary data in the *Event Log*.
Testing	Off	Blinking	Yellow Triangle	Port is performing an internal loopback test.
	On	Blinking	Yellow Triangle	Port is performing an external loopback test.

Repair procedures - EFCM Basic Edition

The following procedures (performed at a PC communicating with the EFCM Basic Edition interface) are described:

- *Obtain log information* on page 160
- *Perform port Diagnostics* on page 165
- *Collect maintenance data* on page 172
- *Set online state* on page 174
- *Block or unblock a port* on page 175
- *Upgrade firmware* on page 176
- *Manage configuration data* on page 178

Obtain log information

The EFCM Basic Edition interface provides access to logs that contain maintenance information.

Select the desired log from the options in the *Logs* menu in the EFCM Basic web interface. Logs with maintenance information are:

- Event.
- Link Incident.
- Audit
- Security

- Open Trunking Re-Route.
- Fabric.
- Embedded Port Frame.
- All
- Syslog Configuration

Event Log

The *Event Log* displays events or errors. Entries reflect the status of the management interface and managed product.

The following information can be obtained from the *event* logs:

- **Date/Time -** The date and time the event occurred.
- **Error Code -** The three-digit code that describes the event. Event codes are listed and described in Appendix A, *Event code tables*.
- **Severity -** The severity of the event (*Informational*, *Minor*, *Major*, or *Severe*).
- **Event Data -** Supplementary information (if available) in hexadecimal format. Event data is described in Appendix A, *Event code tables*.

Link Incident Log

The *Link Incident Log* records Fibre Channel link incident events and causes.

The following information can be obtained from the *link incident* logs:

- **Date/Time -** The date and time the link incident occurred.
- **Port -** The port number that reported the link incident.
- **Link Incident Event -** A brief description of the link incident and cause, including:
  - Implicit incident.
  - Bit-error threshold exceeded.
  - Loss of signal or loss of synchronization.
  - Not-operational primitive sequence received.
  - Primitive sequence timeout.
  - Invalid primitive sequence received for current link state.

Refer to *MAP 0500: Port failure or link incident analysis* for corrective actions.

Audit Log

The audit log displays a history of all configuration changes applied to the product from any source such as Element Manager, SNMP management stations, or host.

The following information can be obtained from the *audit* logs:

- **Date/Time-** The date and time of the change on the product.
- **Source-** Identifies the method employed by the user to make the changes (*Maintenance Port, HTTP, Application Interface, SNMP, Fabric, Embedded Web Server, Fibre Channel Host*, or *Telnet*).
- **Action-** User action that caused the configuration change, such as *offline status*, *port name change*, or *change of address*.
- **User ID-** The IP address of the user causing the log.

Security Log

The security log displays security information.

The following information can be obtained from the *security* logs:

- **Reason-** The reason code for the event.
- **Date and Time-** The date and time that the event occurred. The format is yyyy/mm/dd hh:mm:ss:tt. The last two characters (hundredth of seconds) are needed due to possible higher frequency rate of some of the advanced logs.
- **Trigger level-** The severity level of the event (*Informational, Warning,* or *Fatal*).
- **Count-** The number of times that the same event occurred.
- **Category-** The category of the security event.
- **Description-** The description of the security event.
- **Data**
  - **User Name-** The user associated with the event.
  - **IP-** The IP address of the product.
  - **Role-** The role of the user.
  - **Protocol:** The protocol that was used for the security event.

Open Trunking Re-Route Log

The *Open Trunking Re-Route Log* records interswitch link (ISL) congestion events that cause Fibre Channel traffic to be routed through an alternate ISL. Entries reflect the traffic re-route status at the managed product.

The following information can be obtained from the *Open Trunking Re-Route* logs:

- **Date/Time -** The date and time the re-route occurred.
- **Receive Port -** The target port number (decimal) used for receiving Fibre Channel traffic after the re-route.
- **Target Domain -** The domain ID (decimal) of the target device to which Fibre Channel traffic from the product was rerouted.
- **Old Exit Port -** The product port number (decimal) used for transmitting Fibre Channel traffic before the re-route action.
- **New Exit Port -** The product port number (decimal) used for transmitting Fibre Channel traffic after the re-route action.

Fabric Log

The *Fabric Log* records the time and nature of changes made to a multiswitch fabric. The information is useful for isolating zoning or fabric-wide problems.

The following information can be obtained from the *fabric* logs:

- **Count -** The cumulative count of log entries (wrapping or non-wrapping).
- **Date/Time -** The date and time the change occurred.
- **Description -** The description of the zoning or fabric change.
- **Data -** Supplementary information (if available) in text format.

NOTE: Identical entries are recorded in the wrapping and non-wrapping logs. When the non-wrapping log fills, old records are overwritten. The wrapping log preserves all records.

Embedded Port Frame Log

The *Embedded Port Frame Log* records all Fibre Channel frames transmitted through the product's embedded port, including Class F traffic, fabric logins, state change notifications, and exception frames. The information is useful for Fibre Channel frame debugging (usually performed by second-level support.

The following information can be obtained from the *embedded port frame* logs:

- **Count -** The cumulative count of log entries (wrapping or non-wrapping).

- **Date/Time -** The date and time frame that were transmitted through the embedded port.
- **Port # -** The Fibre Channel port number (decimal) transmitting frame through the embedded port.
- **Direction -** Fibre Channel frame direction - incoming (**I**) or outgoing (**O**).
- **SOF -** The start of frame character (hexadecimal).
- **EOF -** The end of frame character (hexadecimal).
- **Payload Size -** The size of frame payload in bytes.

All logs

This lists down all the logs that were generated from the last time that the logs were cleared. The logs are classified by type and the logs in each type are classified in a chronological order with the latest log entry on top.

The following information can be obtained from the *all* logs:

- Log Type: The type of log (Audit, Event, Security etc.)
  - **Reason-** The reason code for the event.
  - **Date/Time-** The date and time that the event occurred. The format is yyyy/mm/dd hh:mm:ss:tt. The last two characters (hundredth of seconds) are needed due to possible higher frequency rate of some of the advanced logs.
  - **Trigger Level-** The severity level of the event (*Informational*, *Warning*, or *Fatal*).
  - **Count-** The number of times that the same event occurred.
  - **Category-** The category of the security event.
  - **Description-** The description of the security event.
  - **Data-**
    - User Name: The name of the user.
    - IP Address: The IP address of the product.
    - Protocol: The protocol used to generate the log.

Syslog Configuration

Using the Syslog Configuration, you can choose to generate only the types of log that you require.

Click *Enable* to enable Syslogs.

To generate a syslog for a product, use the following steps

1. Click *New.*
2. Type the IP address of the product for which the syslog is to be generated in the *IP address* field.
3. Select a *facility* from the drop down list.
4. Select the logs that you want to generate from the options in the *Logs* section. The following options are available
   - — Event
   - — Open Trunking Re-Route
   - — Link Incident
   - — Threshold Alert
   - — Security
   - — Audit
   - — Fabric
   - — Embedded Port Frame
5. Click *OK* to activate the changes.

Perform port Diagnostics

Fibre Channel port diagnostic information is obtained by:

- Inspecting port properties, predictive optics monitoring (POM) data, or port transceiver technology information at the lower panel of the *Port List* view.
- Inspecting statistical information at the *Performance* view.
- Performing an internal or external loopback test.

Port List View

The EFCM Basic Edition interface provides access to port diagnostic information through the *Port List* view.

To open the *Port List* view, select *Port List* from the *Product* menu (*Product>Port List)*. As an example, the figure shows POM data in the lower panel (Figure 46).

Product > Port List
Jump to Port 1
go
Port
Name
Block Configuration
Operational State
Type
Health Status
Transceiver
0 - Unblocked No Light Gx Port No Info SFP
1 - Unblocked No Light Gx Port Normal SFP
2 - Unblocked No Light Gx Port No Info SFP
3 - Unblocked Not Installed Gx Port No Info Unknown
4 - Unblocked No Light Gx Port No Info SFP
5 - Unblocked No Light Gx Port No Info SFP
6 - Unblocked No Light Gx Port Normal SFP
7 - Unblocked No Light Gx Port No Info SFP
8 - Unblocked Not Installed Gx Port No Info Unknown
9 - Unblocked Not Installed Gx Port No Info Unknown
10 Unblocked Not Installed Gx Port No Info Unknown
Port Number 1
Port Name
Port Type Gx Port
Operating Speed Not Established
Fiber Channel Address N/A
Port WWN 2001080088E2B184
Attached Port WWN/Alias None
i16M2007

Figure 46 Port List View

A row of information for each port appears. Each row consists of the following columns:

Table 22 Port List Table

Port Property	Description
Port	The product port number.
Name	The user-defined name or description for the port.
Block Configuration	Indicates if a port is blocked or unblocked.
Operational State	Port state (*Online*, *Offline*, *Not Installed*, *Inactive*, *Invalid Attachment*, *Link Reset*, *No Light*, *Not Operational*, *Port Failure*, *Segmented E_Port*, or *Testing*).

Table 22 Port List Table

Port Property	Description
Type	The type of port, including generic mixed port (*GX_Port*), fabric mixed port (*FX_Port*), generic port (*G_Port*), fabric port (*F_Port*), or expansion port (*E_Port*).
Health Status	The condition of the installed optical transceiver (*Normal*, *Warning*, *Alarm*, or *No Info*).
Transceiver	Installed transceiver type (*SFP*, *XFP*, or *Unknown*).

Inspect Port Properties

At the *Port List* view, click a physical port number listed in the *Port* column. Physical properties for the selected port appear in the lower panel of the view:

Table 23 Inspect Port Properties Table

Port Property	Description
Port Number	The product's port number.
Port Name	The user-defined name or description for the port.
Port Type	The user-defined port type (*GX_Port*, *FX_Port*, *G_Port*, *F_Port*, or *E_Port*).
Operating Speed	The port operating speed (*Not Established*, *1 Gbps*, *2 Gbps*, or *4 Gbps*)
Fibre Channel Address	The Port FC address identifier. Port FC address if the port was swapped.
Port WWN	The Fibre Channel world wide name (WWN) of the port.
Attached Port WWN	Fibre Channel WWN of the device attached to the port.
Block Configuration	The user-configured state for the port (*Blocked* or *Unblocked*).
Block Reason	The reason for blocking the port.
Beaconing	The user-specified for the port (*On* or *Off*).
FAN Configuration	User-configured state for fabric address notification (FAN) configuration (*Enabled* or *Disabled*).
RX BB Credit	The number of receive BB credits available for the port.
Operational State	The port state (*Online*, *Offline*, *Not Installed*, *Inactive*, *Invalid Attachment*, *Link Reset*, *No Light*, *Not Operational*, *Port Failure*, *Segmented E_Port*, *Disabled*, or *Testing*).
Reason	A summary appears describing the reason if the port state is *Segmented E_Port*, *Invalid Attachment*, or *Inactive*. For any other port state, the reason is *N/A*.

Inspect POM data

At the *Port List* view, click the entry for a port in the *Health Status* column. POM data for the selected port appears in the lower panel of the view (Figure 46):

Table 24 POM Data Table

Port Property	Description
Port Number	The product's port number.
Health Status	The condition of the installed optical transceiver (*Normal*, *Warning*, *Alarm*, or *No Info*).
Transceiver Type	The installed transceiver type (*SFP*, *XFP*, or *Unknown*).

If the port has a digital diagnostics (DD) enabled optical transceiver installed, product firmware displays a table of reported temperature, voltage, current, transceiver power, and receiver power. Optical transceivers also provide vendor-specific threshold values for these parameters.

Inspect port transceiver technology

At the *Port List* view, click the entry for a port in the *Transceiver* column. Port transceiver technology information for the selected port appears in the lower panel of the view:

Table 25 Inspect Port Transceiver Technology Table

Port Property	Description
Port Number	The product's port number.
Identifier	The installed transceiver type (*SFP*, *XFP*, or *Unknown*).
Connector type	The type of port connector (*LC*, *MT_RJ*, *MU*, *Unknown*, or *Internal Port*).
Transceiver	The type of port transceiver (*Shortwave Laser*, *Longwave Laser*, *Long Distance Laser*, *Unknown*, or *None*).
Distance Capability	The port transmission distance (*Short*, *Intermediate*, *Long*, *Very Long*, or *Unknown*).
Media	The type of optical cable used (*Singlemode*, *multimode 50-micron*, *multimode 62.5-micron*, or *Unknown*).
Speed	The operating speed (*Not Established*, *1 Gbps*, *2 Gbps*, or *4 Gbps*).

Performance View

The EFCM Basic Edition interface provides access to port statistics information through the *Performance* view.

To open this view, select *Performance* from the *Product* menu (*Product>Performance*). The following statistical information appears:

Table 26 Performance View Table

Statistics	Description
Traffic Statistics	Port transmit and receive values for frames Four-byte words transmit and receive value for frames Offline sequences transmit and receive value for frames Link resets and link utilization percentage. Time spent using no transmission buffer-to-buffer credit (BB_Credit)
Error Statistics	Number of: Link failures Synchronization and signal losses Discarded frames Invalid transmission words Primitive sequence errors Cyclic redundancy check (CRC) errors Delimiter errors Address identification errors Short frames.
Class 2 Statistics	Number of: 4-byte words transmitted and received Class 2 frames transmitted, received, busied, or rejected.
Class 3 Statistics	Number of: 4-byte words transmitted and received Class 3 frames transmitted, received, or discarded.
Open Trunking Statistics	These statistics include the number of traffic flows rerouted to or from an ISL due to congestion.

Internal loopback test

Follow the procedure in this section to perform an internal loopback test using the EFCM Basic Edition.

An internal loopback test checks internal port, serializer, and deserializer circuitry and checks for the presence of an optical transceiver, but does not check fiber-optic components of the installed transceiver. Operation of the attached device is disrupted during the test.

Notify the customer that a disruptive internal loopback test will be performed. Ensure that the system administrator quiesces Fibre Channel frame traffic through the port and sets the attached device offline.

To perform an internal loopback test using the EFCM Basic Edition, use the following steps:

NOTE: A small form factor pluggable (SFP) optical transceiver must be installed in the port during the test. A device can remain connected during the test.

---

1. Select *Diagnostics* from the *Maintenance* menu (*Maintenance>Ports>Diagnostics*). The *Diagnostics* view appears (Figure 47).

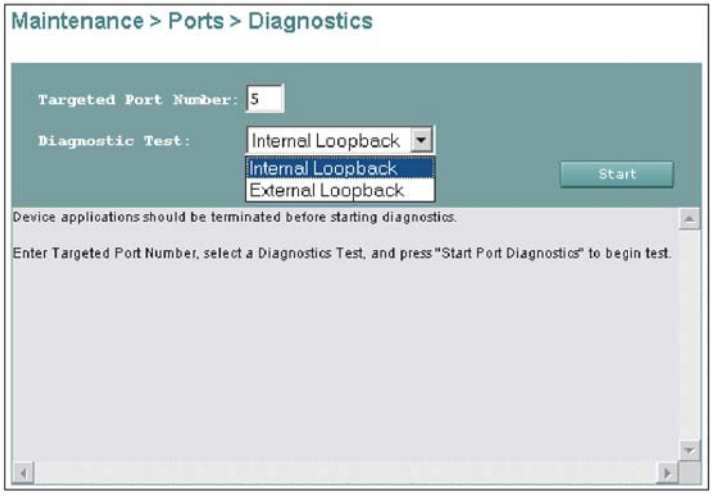

Maintenance > Ports > Diagnostics
Targeted Port Number: 5
Diagnostic Test:
Internal Loopback
Internal Loopback
External Loopback
Start
Device applications should be terminated before starting diagnostics.
Enter Targeted Port Number, select a Diagnostics Test, and press "Start Port Diagnostics" to begin test.
i16M2008

Figure 47 Diagnostics View

2. Type the port number to be tested in the *Targeted Port Number* field.
3. Select the *Internal Loopback* option in the *Diagnostic Test* list box.
4. Click *Start*. The test begins and:
   a. The *Diagnostics* view changes to a *Diagnostics - Executing* view.

b. The message **Diagnostics Time Remaining: xx** appears, where **xx** are the seconds remaining in the test. The test takes approximately 30 seconds.

NOTE: Click *Stop* at any time to abort the loopback test.

5. When the test completes, the *Diagnostics - Executing* view reverts to the *Diagnostics* view. Test results appear as **Passed**, **Failed,** or **Test Incomplete** in the message area of the view.
6. Reset the tested port:
   a. Select *Reset* from the *Maintenance* menu (*Maintenance>Ports>Reset*). The *Reset* view appears.
   b. Select the check box in the *Reset* column corresponding to the tested port.
   c. Click *OK*. The port resets.
7. Notify the customer the test is complete and the attached device can be set online.

External loopback test

Follow the procedures in this section to perform the external loopback test using the EFCM Basic edition.

An external loopback test checks all port circuitry, including fiber-optic components of the installed optical transceiver. To perform the test, the attached device must be quiesced and disconnected from the port, and a singlemode or multimode loopback plug must be inserted in the port.

Notify the customer that a disruptive external loopback test will be performed and the attached device will be disconnected.

To perform an external loopback test using the EFCM Basic Edition interface, use the following steps:

1. Disconnect the fiber-optic jumper cable from the port to be tested.
2. Insert a singlemode or multimode loopback plug into the port receptacle, depending on the port technology.
3. Select *Diagnostics* from the *Maintenance* menu *(Maintenace>Ports>Diagnostics)* in the EFCM Basic interface. The *Diagnostics* view appears (Figure 47).
4. Type the port number to be tested in the *Targeted Port Number* field.

5. Select the *External Loopback* option in the *Diagnostic Test* list box.
6. Click *Start*. The test begins and:
   a. The *Diagnostics* view changes to a *Diagnostics -Executing* view.
   b. The message **Diagnostics Time Remaining: xx** appears, where **xx** are the seconds remaining in the test. The test takes approximately 30 seconds.

   NOTE: Click *Stop* at any time to abort the loopback test.

   When the test completes, the *Diagnostics - Executing* view reverts to the *Diagnostics* view. Test results appear as **Passed**, **Failed,** or **Test Incomplete** in the message area of the view.
7. Remove the loopback plug and reconnect the fiber-optic jumper cable from the device to the port (disconnected in step 1).
8. Reset the tested port:
   a. Select *Reset* from the *Maintenance* menu (*Maintenance>Ports>Reset*). The *Reset* view appears.
   b. Select the check box, next to the tested port, in the *Reset* column.
   c. Click *OK*. The port resets.
9. Notify the customer that the test is complete and the device can be reconnected and set online.

Collect maintenance data

Perform this procedure after a firmware fault or FRU/CRU failure to capture data for analysis by support personnel.

When firmware detects a critical error, the product automatically copies the contents of dynamic random access memory (DRAM) to a dump area in FLASH memory on the CTP card. Maintenance data includes the dump file and engineering logs.

NOTE: An optional full-volatility feature is often required at military sites that process classified data. If the feature is enabled through a product feature enablement (PFE) key, a memory dump file (that may include classified Fibre Channel frames) is not included as part of the data collection procedure.

To collect maintenance data use the following steps:

1. Select *System Files* from the *Maintenance* menu (*Maintenance*>*System Files*). The *System Files* view appears (Figure 48).

Figure 48 System Files View

2. Right-click the *Data Collection* link to open a list of menu options. Select the *Save Target As* menu option. The *Save As* dialog box appears.
3. Insert a blank diskette in the floppy drive of the PC communicating with the EFCM Basic Edition interface.
4. At the *Save As* dialog box, select the floppy drive (**A:**) from the *Save in* drop-down menu, type a descriptive name for the zipped (**.zip**) dump file in the *File name* field, and click *Save*.
5. A *Download* dialog box appears, showing the estimated time remaining to complete the download process. When finished, the dialog box changes to a *Download complete* dialog box.
6. Click *Close* to close the dialog box.
7. Remove the diskette with the newly-collected maintenance data from the PC floppy drive. Return the diskette with the failed CRU to support personnel for failure analysis.

Set online state

This section describes procedures to set the product online or offline. Operational states are:

- **Online -** When the product is set online, an attached device can log in if the port is not blocked. Attached devices in the same zone can communicate with each other.
- **Offline -** When the product is set offline, all ports are set offline and operation of attached Fibre Channel devices is disrupted. The product transmits the OLS to attached devices, and the devices cannot log in.

NOTE: Do not set the product offline unless directed to do so by a procedural step or the next level of support.

To set the product online or offline:

1. Select *Switch* from the *Maintenance* menu (*Maintenance>Switch*). The *Switch* view appears (Figure 49).

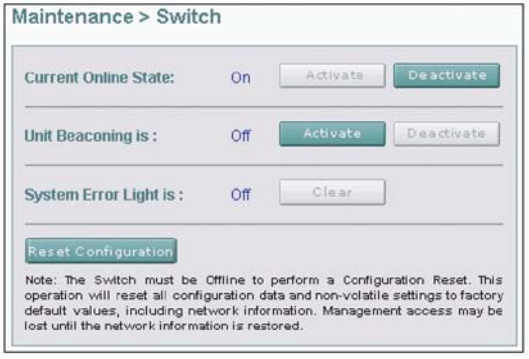

Maintenance > Switch
Current Online State:
On
Activate
Deactivate
Unit Beaconing is :
Off
Activate
Deactivate
System Error Light is :
Off
Clear
Reset Configuration
Note: The Switch must be Offline to perform a Configuration Reset. This operation will reset all configuration data and non-volatile settings to factory default values, including network information. Management access may be lost until the network information is restored.
i16M2010

Figure 49 Switch View

2. Perform one of the following:
   - If the product is offline, click the green *Activate* button adjacent to the *Current Online State:* field. The product comes online.
   - If the product is online, click the green *Deactivate* button adjacent to the *Current Online State:* field. The product goes offline.

Block or unblock a port

Follow the procedures in this section to block or unblock a Fibre Channel port.

Blocking a port prevents an attached device or fabric element from communicating. A blocked port continuously transmits the OLS.

To block or unblock a port using the EFCM Basic Edition, use the following steps:

1. Select *Basic Info* from the *Configure* menu (*Configure>Ports>Basic Info*). The *Basic Information* view appears (Figure 50).

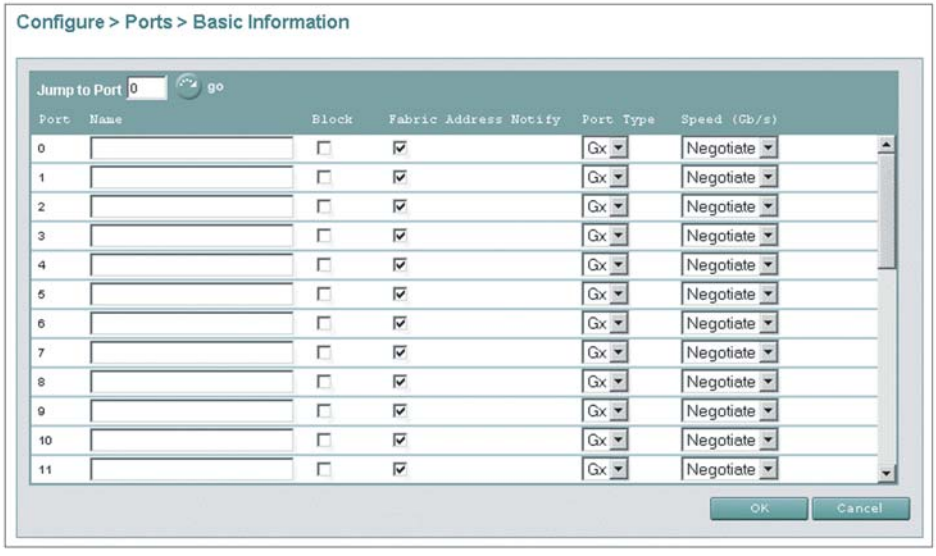

Configure > Ports > Basic Information
Jump to Port 0 go
Port Name Block Fabric Address Notify Port Type Speed (Gb/s)
0 1 2 3 4 5 6 7 8 9 10 11
Gx
Negotiate
OK
Cancel
i16M2011

Figure 50 Basic Information View

2. Use one of the following steps to block or unblock a port:
   - Select the check box for the port to be blocked in the *Blocked* column to block the port. Repeat the step for other ports.
   - Clear the check box for the port to be unblocked in the *Blocked* column. Repeat the step for other ports to be unblocked.
3. Click *OK* to save and activate changes.

Upgrade firmware

Follow the procedures in this section to upgrade firmware using the EFCM Basic Edition interface.

Firmware is the product operating code stored in FLASH memory on the CTP card. Multiple firmware versions can be stored on a PC hard drive and made available for download through the EFCM Basic Edition interface.

- Determine the active firmware version.
- Download a firmware version.

Determine firmware version

To determine a firmware version, select *Hardware* from the *Product* menu (*Product>Hardware*). The *Hardware* view appears. At the bottom of the page, record the firmware version listed in the *Firmware Level* field.

Download firmware version

Ensure that the desired firmware version is obtained from the Filecenter and resident on the hard drive of the PC communicating with the EFCM Basic Edition interface. Refer to *Download firmware* for instructions.

NOTE: When upgrading firmware, follow all procedural information contained in release notes or engineering change (EC) instructions that accompany the version. Such information supplements information provided in this general procedure.

To download a firmware version using EFCM Basic Edition, use the following steps:

1. Select *Firmware Upgrade* from the *Maintenance* menu (*Maintenance>Firmware Upgrade*). The *Firmware Upgrade* view appears (Figure 51).

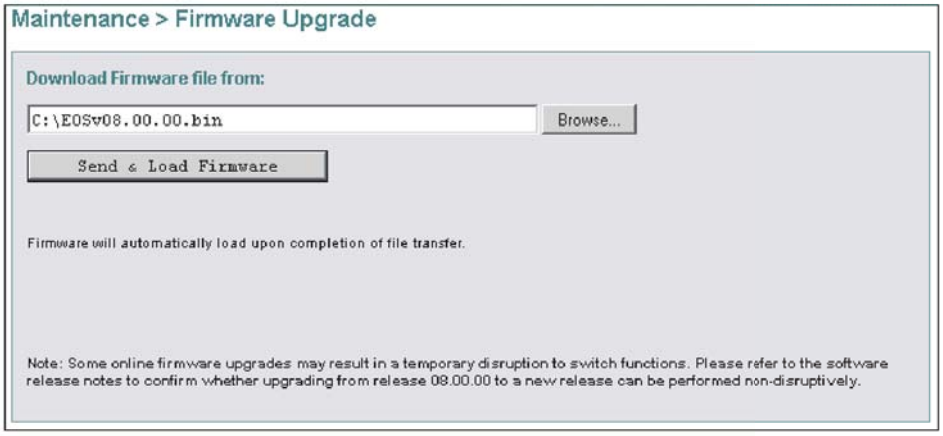

Maintenance > Firmware Upgrade
Download Firmware file from:
C:\EOSv08.00.00.bin
Browse...
Send & Load Firmware
Firmware will automatically load upon completion of file transfer.
Note: Some online firmware upgrades may result in a temporary disruption to switch functions. Please refer to the software release notes to confirm whether upgrading from release 08.00.00 to a new release can be performed non-disruptively.
I16M2012

Figure 51 Firmware Upgrade View

2. Select the desired file from the PC hard drive using the *Browse* button in the *Download Firmware file from* field, or type the desired filename.
3. Click *Send and Load Firmware*. A message box appears, indicating any browser operation will terminate the firmware download.
4. Click *OK* to download firmware. The process takes several minutes to complete, during which the browser is unavailable.

   When the process completes, the message **Firmware successfully received and verified. Your browser connection will be unavailable until unit restart is complete.** appears.

   After verification, the switch performs an initial program load (IPL) that takes approximately 30 seconds to complete. During the IPL, the browser-to-switch Internet connection drops momentarily and the EFCM Basic Edition session is lost.

   After the switch IPL and EFCM Basic Edition session logout, the message **Firmware upgrade complete. Click here to login.** appears.
5. Click **here** to login to the switch and start a new EFCM Basic Edition session. The *Enter Network Password* dialog box appears.
6. Type the default user name and password.

NOTE: The default user name is **Administrator** and the default password is **password.** Both are case-sensitive.

7. Click *OK*. The EFCM Basic Edition interface opens with the *Hardware* view panel displayed.

Manage configuration data

The EFCM Basic Edition interface provides options to:

- Back up and restore the configuration file stored in nonvolatile random-access memory (NV-RAM) on the switch CTP card.
- Reset the configuration file to factory default values.

ATTENTION! The switch must be set offline prior to restoring or resetting the configuration file.

Back up configuration

To back up the switch configuration file to the PC communicating with the EFCM Basic Edition interface use the following steps:

1. Select *Backup Configuration* from the *Maintenance* menu (*Maintenance>Backup Configuration*). The *Backup Configuration* view appears (Figure 52).

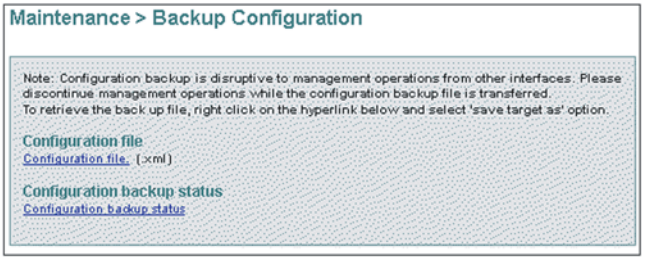

Maintenance > Backup Configuration
Note: Configuration backup is disruptive to management operations from other interfaces. Please discontinue management operations while the configuration backup file is transferred.
To retrieve the back up file, right click on the hyperlink below and select 'save target as' option.
Configuration file
Configuration file (.xml)
Configuration backup status
Configuration backup status
i16M2013

Figure 52 Backup Configuration View

2. Right-click the *Configuration file* link to open a list of menu options. Select the *Save Target As* menu option. The *Save As* dialog box appears.
3. At the *Save As* dialog box, select the hard drive (**C:**) from the *Save in* drop-down menu, type a descriptive name for the extensible markup language (**.xml**) configuration file in the *File name* field, and click *Save*.

4. A *Download* dialog box appears, showing the estimated time remaining to complete the backup process. When finished, the dialog box changes to a *Download complete* dialog box.
5. Click *Close* to close the dialog box.

Restore configuration

Notify the customer that the switch will be set offline. Ensure that the system administrator quiesces Fibre Channel traffic through the switch and sets attached devices offline.

To restore the switch configuration file from the PC communicating with the EFCM Basic Edition interface, use the following steps:

1. Set the switch offline. For instructions, refer to *Set online state*.
2. Select *Restore Configuration* from the *Maintenance* menu (*Maintenance>Restore Configuration*). The *Restore Configuration* view appears (Figure 53).

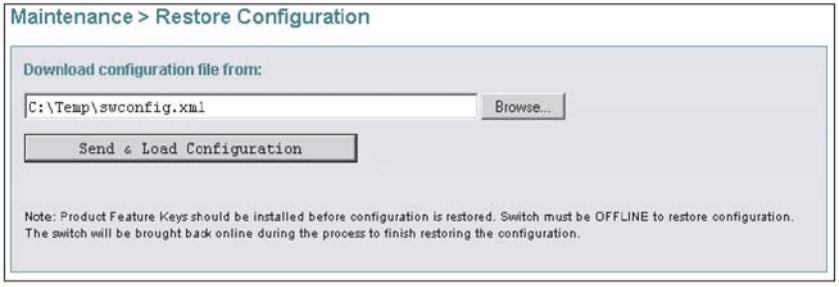

Maintenance > Restore Configuration
Download configuration file from:
C:\Temp\swconfig.xml
Browse...
Send & Load Configuration
Note: Product Feature Keys should be installed before configuration is restored. Switch must be OFFLINE to restore configuration.
The switch will be brought back online during the process to finish restoring the configuration.
i16M2014

Figure 53 Restore Configuration View

3. Select the file from the PC hard drive using the *Browse* button or type the filename at the *Download Configuration file from* field.
4. Click *Send and Load Configuration*. A message box appears, indicating any browser operation will terminate the configuration download.
5. Click *OK* to download the configuration. The process takes several minutes to complete, during which the browser is unavailable. When the process completes, the message **Configuration restored successfully.** is displayed.

Reset configuration data

When configuration data is reset to factory default values, the switch defaults to the factory-set (Internet Protocol) IP address and all optional features are disabled.

Notify the customer that the switch will be set offline. Ensure that the system administrator quiesces Fibre Channel frame traffic through the switch and sets attached FC-AL devices offline.

To reset configuration data to factory defaults using the EFCM Basic edition, use the following steps:

1. Set the switch offline. For instructions, refer to *Set online state*.
2. Select *Switch* from the *Maintenance* menu (*Maintenance>Switch*). The *Switch* view appears (Figure 49).
3. Click *Reset Configuration*. A dialog box with the message **Are you sure that you want to reset the configuration?** appears.
4. Click *OK* to reset the configuration.
5. The switch IP address resets to the default address of **10.1.1.10**.
   - — If the configured IP address (prior to reset) was the same as the default address, the browser-to-switch Internet connection is not affected and the procedure is complete.
   - — If the configured IP address (prior to reset) was not the same as the default address, the browser-to-switch Internet connection drops and the EFCM Basic Edition session is lost. Continue to the next step.
6. To change the switch IP address and restart the EFCM Basic Edition interface, refer to *Configure network information*. To restart the EFCM Basic Edition interface using the default IP address of **10.1.1.10**:
   a. Type the default IP address of **10.1.1.10** as the Internet URL. The *Enter Network Password* dialog box appears.
   b. Type the default user name and password.

      NOTE: The default user name is **Administrator** and the default password is **password.** The user name and password are case-sensitive.

   c. Click *OK*. The EFCM Basic Edition interface opens and the procedure is complete.

Repair procedures - SAN management application

The following procedures (performed at a rack-mount management server running a SAN management application) are described. SAN management applications include SANavigator 4.2 (or later) and EFCM 8.7 (or later).

- *Obtain Fabric Log information* on page 181
- *Obtain Switch Log information* on page 184
- *Perform port diagnostics* on page 190
- *Collect maintenance data* on page 200
- *Set online state* on page 201
- *Block or unblock a port* on page 202
- *Upgrade firmware* on page 203
- *Manage configuration data* on page 206

Obtain Fabric Log information

The SAN management application provides access to logs that contain fabric-level maintenance information. At the application main window, select the *Logs* option from the *Monitor* menu, then click (select) the desired log option.

Logs with maintenance information are:

- Audit
- Event
- Fabric
- Group
- Product Status
- Session
- Security

Audit Log

The audit log displays a history of all configuration changes applied to the product from any source such as Element Manager, SNMP management stations, or host.

The following information can be obtained from the *audit* logs.

- **Date/Time -**The time and date of the log entry.
- **Type:** The type of log entry.
- **Parameter:** Description of the log entry.
- **User:** The user who created the log entry.

Event Log

The *Event Log* records simple network management protocol (SNMP) trap events, client-server communication errors, and other problems recorded by the SAN management application. Information provided is generally intended for use by third-level support personnel to fault isolate significant problems.

The following information can be obtained from the *event* logs.

- **Date/Time -** The date and time the event occurred.
- **Event -** An event number and brief description of the event. Include this information when reporting an event to customer support.
- **Product -** The product associated with the event and configured name or IP address associated with the instance are displayed.
- **Data -** Additional event data for fault isolation. Include this information when fault isolating a call-home problem or reporting an event to customer support.

Fabric Log

The *Fabric Log* records the time and nature of changes made to a multiswitch fabric. The information is useful for isolating zoning or fabric-wide problems.

The following information can be obtained from the *fabric* logs.

- **Date/Time -** The date and time the change occurred.
- **Fabric Event -** The description of the zoning or fabric change.
- **Description -** Supplementary information (if available) in text format.

Group Log

The group log enables users to view and delete the event logs that were created using *Create Group Event* log (*Configure>Group Manager*). The users can use this option to group switchess under a single group name and generate an event log for the entire group.

The following information can be obtained from the *Group* logs:

- **Level-** The severity level of the event.
- **Source-** The name of the product.
- **Type-** The type of event occurred.
- **Description-** The description of the event with the port number of the product causing the event**.**
- **Time-** The time of the event.
- **IP-** The IP address of the server.
- **Node Name-** The name of the product causing the event.
- **Port Name**- The port name of the product.

Product Status Log

The *Product Status Log* records the previous and current status of a managed product, and indicates the instance of an Element Manager application that should be opened to investigate a problem.

The following information can be obtained from the *Product Status* logs:

- **Date/Time -** The date and time the status change occurred.
- **Network Address -** The IP address or configured name of the product. The address or name corresponds to the address or name displayed under the product icon at the physical map.
- **Product ID-** The Product ID of the switch.
- **Previous Status -** The status of the product prior to the change (*Operational*, *Degraded*, *Failed*, *Out of Band Online*, or *Unknown*). An *Unknown* status indicates the SAN management application cannot communicate with the product.
- **New Status -** The status of the product after the change (*Operational*, *Degraded*, *Failed*, *Out of Band Online*, or *Unknown*).

Sessions Log

The sessions log provides information about the different sessions in the fabric.

The following information can be obtained from the sessions logs:

- **Date/time-** The date/time at which the session was established or terminated.
- **Description-** The description of the session.

- **User-** The name of the user who initiated or terminated the session.
- **Network Address-** The network address of the machine hosting the EFCM application from which the session was established or terminated.

Security

The security log displays security information.

The following information can be obtained from the *security* logs:

- **Severity -** The severity level of the event (*Informational, Warning,* or *Fatal*).
- **User-** The user associated with the event.
- **Reason-** The reason code for the event.
- **Description-** The description of the security event.
- **Date and Time-** The date and time that the event occurred. The format is yyyy/mm/dd hh:mm:ss:tt. The last two characters (hundredth of seconds) are needed due to possible higher frequency rate of some of the advanced logs.
- **Count-** The number of times that the same event occurred.
- **Category-** Displays the category that caused the log entry.
- **IP-** The IP address of the product.
- **Role-** The role of the user.
- **Interface-** The interface causing the security event.

Obtain Switch Log information

The Element Manager application provides access to logs that contain switch-level maintenance information.

Select the desired log option from the *Logs* menu in the Element Manager. Logs with maintenance information are:

- Audit.
- Event.
- Hardware.
- Link Incident.
- Port Threshold Alert.

- Open Trunking.
- Embedded Port.
- Switch Fabric.

Audit Log

The audit log displays a history of all configuration changes applied to the product from any source such as Element Manager, SNMP management stations, or host.

The following information can be obtained from the *audit* logs:

- **Date/Time-** The date and time of the change on the product.
- **Action-** User action that caused the configuration change, such as *offline status, port name change*, or *change of address*.
- **Source-** Identifies the user making the change through the product Element manager and IP or DNS host name address of the remote computers running the client software.
- **Identifier-** The user making the change.

Event Log

The *Event Log* records events or errors. Entries reflect the status of the management interface and managed product.

management interface and managed product.

The following information can be obtained from the *event* logs:

- **Date/Time -** The date and time the event occurred.
- **Event -** The three-digit code that describes the event. Event codes are listed and described in Appendix A, *Event code tables*.
- **Description -** A brief description of the event.
- **Severity -** The severity of the event (*Informational*, *Minor*, *Major*, or *Severe*).
- **FRU-Position -** An acronym representing the FRU type, followed by a number representing the FRU chassis position.
- **Event Data -** Supplementary information (if available) in hexadecimal format. Event data is described in Appendix A, *Event code tables*.

Hardware Log

The *Hardware Log* records a history of part removals and replacements (insertions) for the switch.

The following information can be obtained from the *hardware* logs:

- **Date/Time -** The date and time the FRU was inserted or removed.
- **FRU -** An acronym representing the FRU type.
- **Position -** A number representing the FRU chassis position. The chassis (slot) position for a nonredundant CTP card is **0**. Chassis slots for redundant power supplies are **0** and **1**.
- **Action -** The action performed (*Inserted* or *Removed*).
- **Part Number -** The part number of the inserted or removed FRU.
- **Serial Number -** The serial number of the inserted or removed FRU.

Link Incident Log

The following information can be obtained from the Link Incident logs:

- **Date/Time -** The date and time the link incident occurred.
- **Port -** The port number reporting the link incident.
- **Link Incident Event -** Brief description of the link incident and cause, including:
  - — Implicit incident.
  - — Bit-error threshold exceeded.
  - — Loss of signal or loss of synchronization.
  - — Not-operational primitive sequence received.
  - — Primitive sequence timeout.
  - — Invalid primitive sequence received for current link state.

Refer to *MAP 0500: Port failure or link incident analysis* for corrective actions.

Port Threshold Alert Log

The *Port Threshold Alert Log* records a history of threshold alert notifications.

The following information can be obtained from the *Port Threshold Alert* logs:

- **Date/Time -** The date and time the alert occurred.

- **Name -** The alert name as configured using the *Configure Threshold Alerts* dialog box.
- **Port -** The port number where the alert occurred.
- **Type -** The type of alert: transmit (*Tx*) or receive (*Rx*).
- **Utilization % -** The usage of traffic capacity in percent. This setting constitutes the threshold value and is configured through the *Configure Threshold Alerts* dialog box.
  For example, a value of 25 means that the threshold occurs when throughput reaches 25 percent of the port capacity.
- **Interval -** The time interval during which throughput is measured and an alert can generate. Set through the *Configure Threshold Alerts* dialog box.

Security

The security log displays security information.

The following information can be obtained from the *security* logs:

- **Trigger level -** The severity level of the event (*Informational*, *Warning*, or *Fatal*).
- **User-** The user associated with the event.
- **Reason-** The reason code for the event.
- **Description-** The description of the security event.
- **Date and Time-** The date and time that the event occurred. The format is yyyy/mm/dd hh:mm:ss:tt. The last two characters (hundredth of seconds) are needed due to possible higher frequency rate of some of the advanced logs.
- **Count-** The number of times that the same event occurred.
- **Category-** Displays the category that caused the log entry.
- **IP-** The IP address of the product.
- **Role-** The role of the user.
- **Interface-** The interface causing the security event.

Open Trunking Log

The *Open Trunking Log* records ISL congestion events that cause Fibre Channel traffic to be routed through an alternate ISL. Entries reflect the traffic re-route status at the managed product.

The following information can be obtained from the *Open Trunking* logs:

- **Date/Time -** The date and time the re-route occurred.
- **Receive Port -** The target port number (decimal) used for receiving Fibre Channel traffic after the re-route.
- **Target Domain -** The domain ID (decimal) of the target device to which Fibre Channel traffic from the switch was rerouted.
- **Old Exit Port -** The port number (decimal) used for transmitting Fibre Channel traffic before the re-route.
- **New Exit Port -** The port number (decimal) used for transmitting Fibre Channel traffic after the re-route.

Embedded Port Log

The *Embedded Port Log* records all Fibre Channel frames transmitted through the product's embedded port, including Class F traffic, fabric logins, state change notifications, and exception frames. The information is useful for Fibre Channel frame debugging (usually performed by second-level support).

The following information can be obtained from the *Embedded Port* logs:

- **Date/Time -** The date and time frame was transmitted through the embedded port.
- **Port -** The Fibre Channel port number (decimal) used for transmitting frame through the embedded port.
- **Direction -** The Fibre Channel frame direction (*In* or *Out*).
- **Frame Header -** 24-byte frame header (hexadecimal).
- **Length -** The size of frame payload in bytes.
- **Payload -** The first 32 bytes of frame payload (hexadecimal).
- **SOF -** The start of frame character (hexadecimal).
- **EOF -** The end of frame character (hexadecimal).

NOTE: Identical entries are recorded in the wrapping and non-wrapping logs. When the non-wrapping log fills, old records are overwritten. The wrapping log preserves all records.

Switch Fabric Log

The *Switch Fabric Log* records the time and nature of changes made to a multiswitch fabric that affect this product.

The following information can be obtained from the *Switch Fabric* logs:

- **Date/Time -** The date and time the change occurred. Timing granularity is provided to one hundredth of a second.
- **Description -** The description of the zoning or fabric change.
- **Event Data -** Supplementary event data that provides additional information that varies according to the even logged.
- **Ports (RSCN only) -** The list of product ports affected by registered state change notifications (RSCNs) related to the event.

NOTE: Identical entries are recorded in the wrapping and non-wrapping logs. When the non-wrapping log fills, old records are overwritten. The wrapping log preserves all records.

Syslog Configuration

Using the Syslog Configuration, you can choose to generate only the required types of logs.

The syslog configuration option displays the *Syslog Configuration* dialog box. This dialog box has two tabs (*Recipients/Logs*).

To enable syslog transmitting, click the *Enable syslog transmitting* check box. If the firmware does not support syslog, a message appears saying that this feature is not supported in this release.

- **Recipients Tab-** The Recipients tab displays the number of IP Address rows that are supported by the firmware.
  - — **IP Address-** Type the IP Address for the device that is to receive the log information. Type in a new IP address or edit an existing IP address.
  - — **Facility-** Select a facility from the dropdown list.
  - — Click the *Activate* button to validate the IP address.
- **Logs Tab-** The Logs tab displays a check box for each log that the firmware supports for generating syslog messages. Selecting (checking) a log causes the firmware to generate a syslog event each time an entry is added to the log.
  - — **Event-** Select (check) box to include Event log.
  - — **Audit-** Select (check) box to include Audit log.

— **Link incident-** Select (check) box to include Link Incident log.

— **Threshold alert-** Select (check) box to include Threshold Alert log.

— **Security-** Select (check) box to include Security log.

— **Embedded port-** Select (check) box to include Embedded Port log.

— **Fabric-** Select (check) box to include Fabric log.

— **Open Trunking-** Select (check) box to include Open Trunking log.

Perform port diagnostics

Fibre Channel port diagnostic information is obtained by:

- Inspecting properties at the *Port List* view.
- Inspecting statistical information at the *Performance* view.
- Inspecting parameters at the *Port Properties* dialog box.
- Inspecting parameters at the *Port Technology* dialog box.
- Performing an internal or external loopback test.
- Swapping ports.

Port List View

The Element Manager application provides access to port diagnostic information through the *Port List* view. To open the *Port List* view, click the *Port List* tab in the Element Manager (Figure 54).

A row of information for each port appears. Each row consists of the following columns:

- **Port # -** The product's port number.
- **FC Address -** The logical port address (hexadecimal format).
- **Name -** The user-defined name or description for the port.

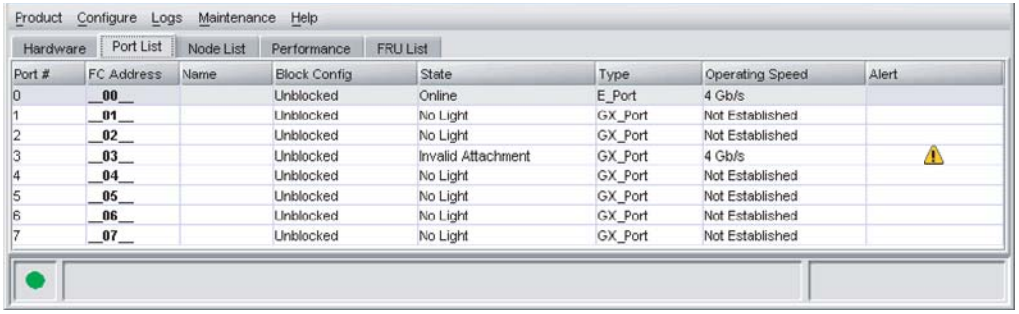

Product Configure Logs Maintenance Help
Hardware Port List Node List Performance FRU List
Port # FC Address Name Block Config State Type Operating Speed Alert
0 __00__ Unblocked Online E_Port 4 Gb/s
1 __01__ Unblocked No Light GX_Port Not Established
2 __02__ Unblocked No Light GX_Port Not Established
3 __03__ Unblocked Invalid Attachment GX_Port 4 Gb/s
4 __04__ Unblocked No Light GX_Port Not Established
5 __05__ Unblocked No Light GX_Port Not Established
6 __06__ Unblocked No Light GX_Port Not Established
7 __07__ Unblocked No Light GX_Port Not Established
i16M2015

Figure 54 Port List View

- **Block Config -** Indicates if a port is blocked or unblocked.
- **State -** The port state (*Online*, *Offline*, *Not Installed*, *Inactive*, *Invalid Attachment*, *Link Reset*, *No Light*, *Not Operational*, *Port Failure*, *Segmented E_Port*, or *Testing*).
- **Type -** The type of port (*GX_Port*, *FX_Port*, *G_Port*, *F_Port*, or *E_Port*).
- **Operating Speed -** The operating speed of the port (*Not Established*, *1 Gbps*,*2 Gbps*, or *4 Gbps*).
- **Alert -** If link incident (LIN) alerts are configured, a yellow triangle appears in the column when a link incident occurs. A yellow triangle also appears if beaconing is enabled. A red and yellow diamond appears if the port fails.

Performance View

The Element Manager application provides access to port statistics information through the *Performance* view. To open the *Performance* view, click the *Performance* tab.

Bar graphs at the top of the view display instantaneous transmit or receive activity level for each port. The relative value displayed is the greater of the transmit or receive activity. Each graph has 20 green-bar level indicators corresponding to 5% of maximum port throughput. If any activity is detected, at least one green bar appears. A red indicator on each bar graph (high-water mark) remains at the highest level reached since the port was set online. In addition, the following statistical information appears:

Table 27 Statistical Information in Performance View

Statistics Class	Description
Class 2	Number of • 4-byte words transmitted and received • Class 2 frames transmitted, received, busied or rejected
Class 3	Number of • 4-byte words transmitted and received • Class 3 frames transmitted, received, busied or rejected
Error	Number of: • Link Failures • Synchronization and signal losses • Discarded frames • Invalid transmission words • CRC • Delimiter • Address identification errors • Short frames
Operational	Number of • Offline Sequences • Link resets transmitted and received
Traffic	• Port transmit and receive value for frames • Four byte words received and transmitted • Link utilization in percentage • Number of traffic flows rerouted to or from an ISL due to congestion

Port Properties dialog box

To open the *Port Properties* dialog box (Figure 55), double-click a port graphic at the *Hardware* view or a port row at the *Port List* view.

The dialog box provides the following information:

Table 28 Port Properties Table

Port Property	Description
Port Number	The product's port number.
Port Name	The user-defined name or description for the port.
Type	The port type (*E_Port, F_Port, or G_Port).*
Technology	The type of port transceiver and optical cable installed.
Operating Speed	The operating speed of the port (*Not Established, 2 Gbps, or 10 Gbps*).
Fibre Channel Address	The logical port address (hexadecimal format). Not applicable for E_Ports.
Port WWN	The Fibre Channel WWN of the port.
Attached Port WWN	The Fibre Channel WWN of the device attached to the port.
Attached Port Nickname	The alternate name for the node logged into the port.
Block Configuration	A user-configured state for the port (*Blocked* or *Unblocked*).
Rx BB_Credits Configured	The user-defined number of receive BB_Credits allocated to the port.
NPIV Login Limit Configured	The user-defined maximum number of virtual addresses assigned to the physical port when N_Port ID virtualization (NPIV) enabled.
Logged in IDs	The number of virtual addresses logged in to the physical port.
LIN Alerts Configuration	A user-specified state for the port (*On* or *Off*).
FAN Configuration	A user-configured state for FAN configuration (*Enabled* or *Disabled*).
Beaconing	User-specified for the port (*On* or *Off*). When beaconing is enabled, a yellow triangle appears adjacent to the status field.
Link Incident	If no link incidents are recorded, ***None*** appears in the status field. If a link incident is recorded, a summary appears describing the incident, and a yellow triangle appears adjacent to the status field.

Table 28 **Port Properties Table**

Port Property	Description
Operational State	The state of the port (*Online*, *Offline*, *Beaconing*, *Invalid Attachment*, *Link Incident*, *Link Reset*, *No Light*, *Not Operational*, *Port Failure*, *Segmented E_Port*, or *Testing*). A yellow triangle appears adjacent to the status field if the port is in a non-standard state that requires attention. A red and yellow diamond appears adjacent to the status field if the port fails.
Reason	A summary appears describing the reason if the port state is *Segmented E_Port*, *Invalid Attachment*, or *Inactive*. For any other port state, the reason field is blank or *N/A*.
Threshold Alert	If a threshold alert exists for the port, an alert indicator (yellow triangle) and the configured name for the alert appear.
Zoning Enforcement	The zoning policy enforced (*Hard Zoning*, *Soft Zoning*, or *N/A*).

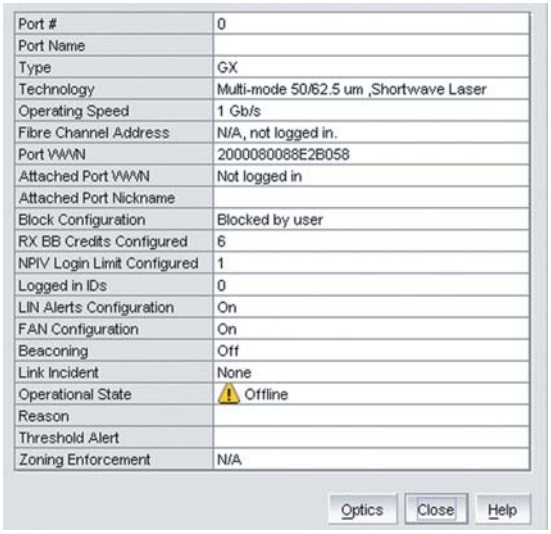


Figure 55 **Port Properties dialog box**

Port Technology dialog box

To open the *Port Technology* dialog box (Figure 56), right-click a port graphic at the *Hardware* view or a port row at the *Port List* view, then select *Port Technology* from the pop-up menu.

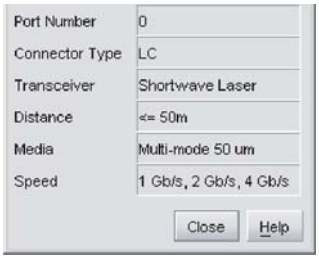


Figure 56 Port Technology dialog box

The dialog box provides the information described in Table 29. The extended information provides G-bic details

Table 29 Port Technology Table

Port Property	Description
Port Number	The director's port number.
Connector type	Type of port connector (*LC*, *Unknown*, or *Internal Port*).
Transceiver	Type of port transceiver (*Shortwave Laser*, *Longwave Laser*, *Long Distance Laser*, *Unknown*, or *None*).
Distance	Port transmission distance (*<=50m*, *50M - 2k*, 2k - 10k, 10k=>).
Media	Type of optical cable used (*Singlemode*, *multimode 50-micron*, *multimode 62.5-micron*, or *Unknown*).
Speed	Operating speed (*Not Established, 2 Gbps, or 10 Gbps*).
Extended Information	
Extended ID	The Extended ID
Vendor Name	The vendor manufacturing the G bic.
Vendor Part #	The vendor part number.
Revision	The revision number.
Serial #	The serial number.
Date Code	The date.
Fiber used and Maximum length	Shows link lengths that are possible based on the fiber type installed. Fields are blank if data is not available.

Internal loopback test

The procedure in this section describes how to perform an internal loopback test using the Element Manager.

An internal loopback test checks internal port, serializer, and deserializer circuitry and checks for the presence of an optical transceiver, but does not check fiber-optic components of the installed transceiver. Operation of the attached device is disrupted during the test.

Notify the customer that a disruptive internal loopback test will be performed. Ensure that the system administrator quiesces Fibre Channel frame traffic and sets attached devices offline.

To perform an internal loopback test using the Element Manager, use the following steps:

NOTE: A small form factor pluggable (SFP) optical transceiver must be installed in the port during the test. A device can remain connected during the test.

---

1. Select *Port Diagnostics* from the *Maintenance* menu (*Maintenance>Port Diagnostics*). The *Port Diagnostics* dialog box appears (Figure 57).
2. Type the port number to be tested or select all ports at the *Port Select* area of the dialog box.
3. Select the *Internal Loop* option from the *Diagnostics Test* list box.
4. Click *Next*. The message **Press START TEST to begin diagnostics** appears, and the *Next* button changes to a *Start Test* button.

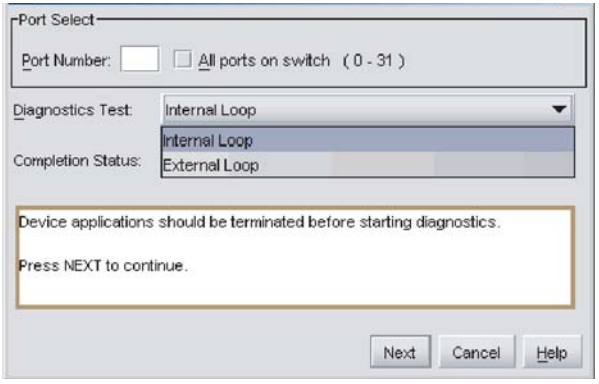


Figure 57 Port Diagnostics dialog box

5. Click *Start Test*. The test begins and:
   a. The *Start Test* button changes to a *Stop Test* button.
   b. The message **Port xx: TEST RUNNING** appears.
   c. A red progress bar (indicating percent completion) travels from left to right across the *Completion Status* field.

   When the test completes, results appear as **Port xx: Passed!** or **Port xx: Failed!** in the message area of the dialog box.
6. When finished, click *Cancel* to close the *Port Diagnostics* dialog box.
7. Reset the port:
   a. Right-click the port graphic on the *Hardware* view. A pop-up menu appears.
   b. Select *Reset Port*. A message box appears, indicating a link reset will occur.
   c. Click *OK*. The port resets.
8. Notify the customer the test is complete and the attached device can be set online.

External loopback test

Follow the procedure in this section to perform an external loopback test using Element Manager.

An external loopback test checks all port circuitry, including fiber-optic components of the installed optical transceiver. To perform the test, the attached device must be quiesced and disconnected from the port, and a singlemode or multimode loopback plug must be inserted in the port.

Notify the customer that a disruptive external loopback test will be performed and the attached device must be disconnected.

To perform an external loopback test using Element Manager application, use the following steps:

1. Disconnect the fiber-optic jumper cable from the port to be tested.
2. Depending on the port technology, insert a singlemode or multimode loopback plug into the port receptacle.
3. Select *Port Diagnostics* from the *Maintenance* (*Maintenance>Port Diagnostics*) menu. The *Port Diagnostics* dialog box appears (Figure 57).

4. Type the port number to be tested or select all ports at the *Port Select* area of the dialog box.
5. Select the *External Loop* option in the *Diagnostics Test* list box.
6. Click *Next*. At the *Port Diagnostics* dialog box, the message **Loopback plug(s) must be installed on ports being diagnosed** appears.
7. Ensure that a loopback plug is installed and click *Next*. The message **Press START TEST to begin diagnostics** appears, and the *Next* button changes to a *Start Test* button.
8. Click *Start Test*. The test begins and:
   a. The *Start Test* button changes to a *Stop Test* button.
   b. The message **Port xx: TEST RUNNING** appears.
   c. A red progress bar (indicating percent completion) travels from left to right across the *Completion Status* field.

   When the test completes, results appear as **Port xx: Passed!** or **Port xx: Failed!** in the message area of the dialog box.
9. When finished, click *Cancel* to close the *Port Diagnostics* dialog box.
10. Remove the loopback plug and reconnect the fiber-optic jumper cable from the device to the port (disconnected in step 1).
11. Reset the port:
    a. At the *Hardware* view, right-click the port graphic. A pop-up menu appears.
    b. Select *Reset Port*. A message box appears, indicating a link reset will occur.
    c. Click *OK*. The port resets.
12. Notify the customer the test is complete and the device can be reconnected and set online.

Swap ports

Follow the procedures in this section to swap the logical port address of the failed port to a known operational port.

Failure of port circuitry behind an optical transceiver may require swapping the logical port address of the failed port to a known operational port. This ensures the port address matches information in the hardware configuration definition (HCD) of an attached host.

Notify the customer that a port swap will be performed. Ensure that the system administrator quiesces Fibre Channel frame traffic through the ports, varies any attached host offline, and sets any attached device offline.

NOTE: This procedure swaps hexadecimal logical port addresses, not decimal port numbers.

To swap the logical port address of the failed port to a known operational port using the Element Manager, use the following steps:

1. Select *Swap Ports* from the *Maintenance* menu *(Maintenance>Port Swapping)*. The *Swap Ports* dialog box appears (Figure 58).
2. Select the radio button associated with the product management style and enter the decimal port numbers (open systems style) or hexadecimal port addresses (FICON style) of the ports to be swapped. The *FC Address* fields update dynamically.
3. Click *Next*. The *Instructions* section of the dialog box indicates the ports will be blocked.

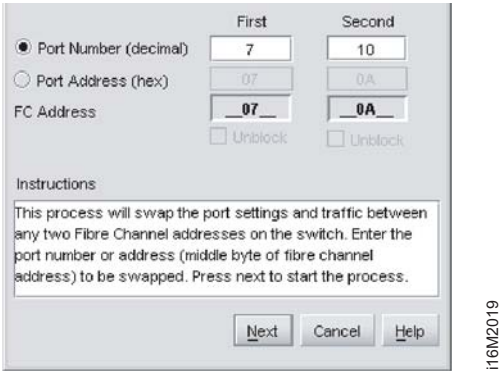


Figure 58 Swap Ports dialog box

4. Click *Next*. Beaconing is enabled for both ports and both ports are blocked. Swap the port fiber-optic cables as directed by the customer's system administrator.
5. Click *Next*. The *Instructions* section of the dialog box indicates the port swap operation is complete and beaconing is disabled. Clear each *Unblock* check box to unblock the ports, then click *Finish*.

6. Ensure that the customer's system administrator varies any attached host online and sets any attached device online.
7. Back up the product configuration data. Refer to *Back up configuration* for instructions.

Collect maintenance data

Perform this procedure after a firmware fault or FRU failure to capture data for analysis by support personnel. Maintenance data includes the dump file and engineering logs.

When firmware detects a critical error, the product automatically copies the contents of DRAM to a dump area in FLASH memory on the CTP card.

NOTE: An optional full-volatility feature is often required at military sites that process classified data. If the feature is enabled through a PFE key, a memory dump file (that may include classified Fibre Channel frames) is not included as part of the data collection procedure.

To collect maintenance data using Element Manager, use the following steps:

1. Select *Data Collection* from the *Maintenance* menu (*Maintenance>Data Collection*). The *Save Data Collection* dialog box appears (Figure 59).

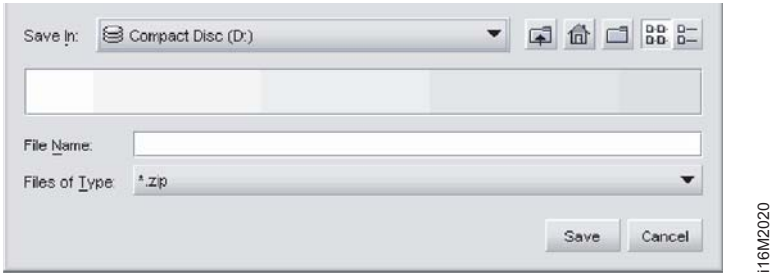


Figure 59 Save Data Collection dialog box

2. Remove the backup CD from the management server's compact disk-rewritable (CD-RW) drive and insert a blank rewritable CD.

3. Select the compact disc drive (**D:**) from the *Look in* drop-down menu at the *Save Data Collection* dialog box. Type a descriptive name for the collected maintenance data in the *File name* field, then click *Save*.
4. The *Data Collection* dialog box appears with a progress bar that shows percent completion of the data collection process. When the process reaches 100%, the *Cancel* button changes to a *Close* Button.
5. Click *Close* to close the dialog box.
6. Remove the CD with the newly-collected maintenance data from the management server's CD-RW drive. Return the CD with the failed CRU to support personnel for failure analysis.
7. Replace the original backup CD in the management server's CD-RW drive to ensure that the backup application operates normally.

Set online state

This section describes procedures to set the product online or offline. These operating states are described as:

- **Online -** When the product is set online, an attached device can log in if the port is not blocked. Attached devices in the same zone can communicate with each other.
- **Offline -** When the product is set offline, all ports are set offline and operation of attached Fibre Channel devices is disrupted. The product transmits the OLS to attached devices, and the devices cannot log in.

NOTE: Do not set the product offline unless directed to do so by a procedural step or the next level of support.

To set the product online or offline using Element Manager, use the following steps:

1. Select *Set Online State* from the *Maintenance* menu (*Maintenance>Set Online State*). The *Set Online State* dialog box appears (Figure 60).

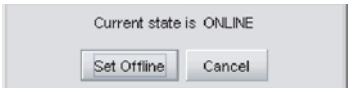


Figure 60 Set Online State dialog box

2. Perform one of the following to set the product online or offline:
   - Click *Set Online*. A warning dialog box appears with the current status of the director as online or offline. Click *OK*.
   - Click *Set Offline*. A warning dialog box appears with the current status of the director as online or offline. Click *OK*.

Block or unblock a port

Follow the procedure in this section to block or unblock a Fibre Channel port using the Element Manager.

Blocking a port prevents an attached device or fabric element from communicating. A blocked port continuously transmits the OLS.

To block or unblock a port or port card using the Element Manager, use the following steps:

1. Click the *Hardware* tab. The *Hardware* view for the selected switch appears.
2. Move the cursor over the port to be blocked or unblocked and right-click the mouse to open a list of menu options.
3. Perform one of the following:
   - **To block a port:** Select the *Block Port* menu option. A *Warning* dialog box appears. Click *OK*. The dialog box closes and the following occur to indicate the port is blocked and offline:
     - At the product, the green port LED extinguishes.
     - At the *Hardware* view, the emulated green port LED extinguishes.
     - A check mark appears adjacent to the *Block Port* menu option.

— **To unblock a port:** Select the *Block Port* menu option. Note the check mark in the box adjacent to the menu item, indicating the port is blocked. A *Warning* dialog box appears. Click *OK*. The dialog box closes and the following occur to indicate the port is unblocked and online:

- At the product, the green port LED illuminates.
- At the *Hardware* view, the emulated green port LED illuminates.
- The box adjacent to the *Block Port* menu option becomes blank.

Upgrade firmware

Firmware is the product operating code stored in FLASH memory on the CTP card. Up to 32 firmware versions can be stored on the management server hard drive and made available for download through the Element Manager application.

To upgrade the firmware using Element Manager, use the following steps:

- Determine the active firmware version for the product.
- Add a firmware version to the management server library.
- Download a firmware version to the product.

Determine firmware version

To determine a switch firmware version, use the following steps:

1. Select *Firmware Library* from the *Maintenance* menu (*Maintenance>Firmware Library*). The *Firmware Library* dialog box appears (Figure 61).

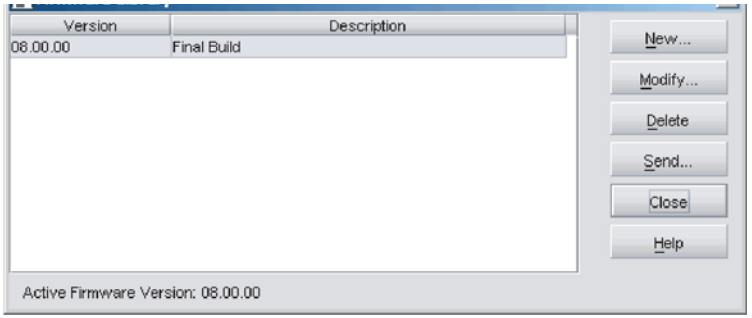


Figure 61 Firmware Library dialog box

2. The active firmware version appears at the lower left corner of the dialog box in ***XX.YY.ZZ*** format, where ***XX*** is the version level, ***YY*** is the release level, and ***ZZ*** is the patch level.
3. Click *Close* to close the dialog box.

Add firmware version to management server library

Ensure that the desired firmware version is obtained from the Filecenter and resident on the management server hard drive. Refer to *Download firmware* for instructions.

NOTE: When upgrading firmware, follow all procedural information contained in release notes or EC instructions that accompany the version. Such information supplements information provided in this general procedure.

To add a firmware version to the management server library using Element Manager, use the following steps:

1. Select *Firmware Library* from the *Maintenance* menu (*Maintenance>Firmware Library*). The *Firmware Library* dialog box appears (Figure 61).
2. Click *New*. The *New Firmware Version* dialog box appears.
3. Select the desired firmware version file (downloaded to the management server hard drive). Ensure that the correct filename appears in the *File name* field and click *Save*. The *New Firmware Description* dialog box appears.

4. Enter a description (up to 24 characters) for the new firmware version. The description should include the installation date and text that uniquely identifies the firmware version. Click *OK*. A *File Transfer* message box appears. A progress bar travels across the message box to show percent completion.

   Upon completion, the *File Transfer* message box converts to a *Transfer Complete* message box, indicating the new firmware version is stored on the management server hard drive. Click *Close* to close the message box.

   The new firmware version and associated description appear in the *Firmware Library* dialog box.

5. Click *Close* to close the dialog box.

6. To send the firmware version, refer to *Download firmware version*.

Download firmware version

To download a firmware version using Element Manager, use the following steps:

1. Before downloading firmware version ***XX.YY.ZZ***, ensure version ***XX.YY.ZZ*** or higher of the SAN management application is running on the server.

   a. Select the *About* option from the *Help* menu. The *About* dialog box appears the SAN management application version. Click *Close* to close the dialog box.

   b. If required, install the correct version of the application. For instructions, refer to *Install or upgrade software*.

2. Perform the data collection procedure as a precaution to preserve switch configuration information. For instructions, refer to *Collect maintenance data*.

3. Select *Firmware Library* from the *Maintenance* menu. The *Firmware Library* dialog box appears (Figure 61).

4. Highlight the firmware version to be downloaded and click *Send*. The send function verifies existence of certain switch conditions before the download process begins. If an error occurs, a message appears indicating the problem must be fixed before the firmware download. Conditions that terminate the process include:

   — A firmware version is being installed to by another user.

   — The switch-to-management server link failed or timed out.

If a problem occurs and a corresponding message appears, go to *MAP 0000: Start MAP* to isolate the problem. If no error occurs, a *Warning* dialog box appears confirming the operation.

5. Click *Yes* to download the firmware version. The *Send Firmware* dialog box appears and the following occur during the download process:
   a. As the download begins, a **Writing data to FLASH** message appears at the top of the dialog box.
   b. As the download progresses, a **Sending Files** message appears and remains as a progress bar shows percent completion of the download. The bar progresses to 100% when the last file is transmitted to the CTP card.
   c. As the download finishes, a **Writing data to FLASH** message appears again.
   d. The switch performs an IPL, during which an **IPLing** message appears at the *Send Firmware* dialog box. In addition, the switch-to-management server Ethernet link drops momentarily.
6. After the IPL, a **Send firmware complete** message appears at the *Send Firmware* dialog box.
7. Click *Close* to close the dialog box.
8. Click *Close* to close the *Firmware Library* dialog box.

Manage configuration data

The Element Manager application provides options to:

- Back up and restore the configuration file stored in NV-RAM on the switch CTP card.
- Reset the configuration file to factory default values.

The switch must be set offline prior to restoring or resetting the configuration file.

Back up configuration

To back up the switch configuration file to the management server using Element Manager, use the following steps:

1. Select *Backup & Restore Configuration* from the *Maintenance* menu. The *Backup and Restore Configuration* dialog box appears (Figure 62).

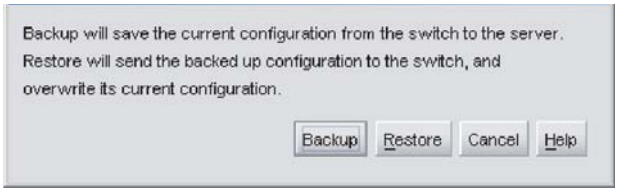

Backup will save the current configuration from the switch to the server.
Restore will send the backed up configuration to the switch, and
overwrite its current configuration.
Backup
Restore
Cancel
Help
i16M2023

Figure 62 **Backup and Restore Configuration dialog box**

2. Click *Backup*. An *Information* dialog box appears, indicating the backup was initiated.
3. Click *OK* to complete the backup and close the dialog box.

Restore configuration

Notify the customer that the switch will be set offline. Ensure that the system administrator quiesces Fibre Channel traffic through the switch and sets attached FC-AL devices offline.

To restore the configuration file from the Element Manager, use the following steps:

1. Set the switch offline. For instructions, refer to *Set online state*.
2. Select *Backup & Restore Configuration* from the *Maintenance* menu (*Maintenance>Backup&Restore Configuration)*. The *Backup and Restore Configuration* dialog box appears (Figure 62).
3. Click *Restore*. A *Warning* dialog box appears, indicating the existing configuration file is to be overwritten.
4. Click *Yes*. A *Restore* dialog box appears, indicating the restore is in progress.

   The *Restore* dialog box displays a **Restore complete** message.
5. Click *Close* to close the dialog box.

Reset configuration data

When configuration data is reset to factory default values, the switch defaults to the factory-set (Internet Protocol) IP address and all optional features are disabled.

Notify the customer that the switch will be set offline. Ensure that the system administrator quiesces Fibre Channel frame traffic through the switch and sets attached FC-AL devices offline.

To reset configuration data to the factory defaults using the Element Manager, use the following steps:

1. Set the switch offline. For instructions, refer to *Set online state*.
2. Select *Reset Configuration* from the *Maintenance* menu (*Maintenance> Reset Configuration*). The *Reset Configuration* dialog box appears (Figure 63).

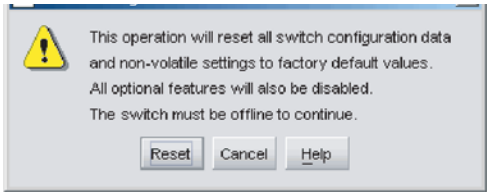

This operation will reset all switch configuration data
and non-volatile settings to factory default values.
All optional features will also be disabled.
The switch must be offline to continue.
Reset
Cancel
Help
i16M2024

Figure 63 Reset Configuration dialog box

3. Click *Reset* to initiate the reset operation and close the dialog box.

   The switch IP address resets to the default address of **10.1.1.10**.

   — If the configured IP address (prior to reset) was the same as the default address, the switch-to-management server Ethernet link is not affected and the procedure is complete.

   — If the configured IP address (prior to reset) was not the same as the default address, the switch-to-management server Ethernet link drops and server communication is lost. Continue to the next step.

4. To *change* the switch IP address and restart the management server session, go to step 5. Restart the management server session using the default IP address of **10.1.1.10**:

   a. Close the Element Manager application and return to the SAN management application.

   b. A grey square with a yellow exclamation mark appears adjacent to the icon representing the reset switch, indicating switch is not communicating with the management server.

   c. At the SAN management application, select *Setup* from the *Discover* menu. The *Discover Setup* dialog box appears (Figure 64).

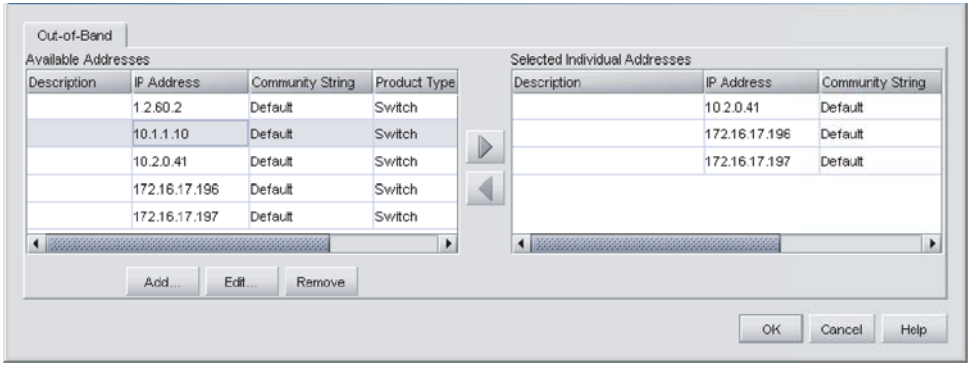


Figure 64 Discover Setup dialog box

d. Select (highlight) the entry representing the reset switch in the *Available Addresses* window and click *Edit*. The *Address Properties* dialog box appears (Figure 65).

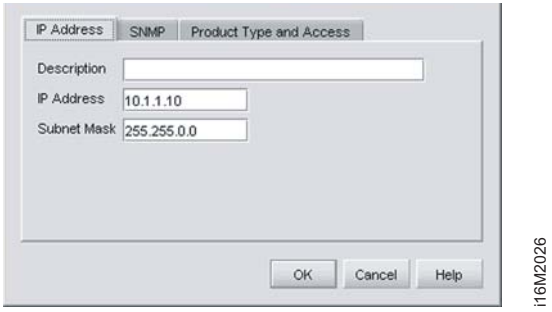


Figure 65 Address Properties dialog box

e. Type **10.1.1.10** in the *IP Address* field and click *OK*. Entries at the *Discover Setup* dialog box reflect the new IP address.

f. Click *OK* at the *Discover Setup* dialog box. Switch-to-management server communication is restored and the procedure is complete.

5. Change the switch IP address and restart the management server session as follows:

a. A grey square with a yellow exclamation mark appears adjacent to the icon representing the reset switch, indicating switch is not communicating with the management server.

b. Delete the icon representing the reset switch. At the SAN management application, select *Setup* from the *Discover* menu. The *Discover Setup* dialog box appears (Figure 64).

c. Select (highlight) the entry representing the reset switch in the *Available Addresses* window and click *Remove*.

d. Click *OK* on the *Discover Setup* dialog box. The switch is no longer defined to the management server.

e. Change the switch IP address through the maintenance port. Refer to *Task 5: Configure product network information (optional)* for instructions.

f. Identify the switch to the SAN management application. Refer to *Task 12: Configure the product to the management application* for instructions.

Install or upgrade software

The firmware version shipped with the product is provided on the *System Version XX.YY.ZZ* CD-ROM. The SAN management application (software) shipped with the product is provided on the *EFC Management Applications* CD-ROM. Subsequent (upgrade) firmware and software versions are provided to customers through IBM.

NOTE: When upgrading firmware or software, follow all procedural information contained in release notes or engineering change (EC) instructions that accompany the version. Such information supplements information provided in this general procedure.

To obtain the latest level of firmware, go to: http://www.ibm.com/servers/storage/support/san/index.html. Locate the link for this switch and then select the link for downloading firmware.

Follow the instructions for downloading the firmware.

1. Transfer the downloaded firmware file to the rack-mount management server or PC communicating with the EFCM Basic Edition interface. Use a diskette, CD-ROM, or other electronic means.
2. From there, install the firmware as described in this guide.

When upgrading software, follow all procedural information contained in release notes or EC instructions that accompany the version. Such information supplements information provided in this general procedure.

To install or upgrade the SAN management application use the following steps:

1. Close and exit all applications on the server.
   - — Insert the *EFC Management Applications* CD-ROM into the CD-ROM drive of the management server.
   - — Ensure that the desired software version is obtained from the Filecenter and resident on the server hard drive. Refer to *Install or upgrade software* for instructions.
2. Open the *Run* dialog box on the Windows PC using *Start>Run*.
3. In the *Open* field at the *Run* dialog box, type:
   - — **`C:\mcdataServerInstall.exe`** to install from the server hard drive.
   - — **`D:\mcdataServerInstall.exe`** to install from the *EFC Management Applications* CD-ROM.
4. Click *OK*. The *InstallShield* third-party application prepares to install the software version, and opens the *InstallShield Wizard* dialog box (Figure 66).

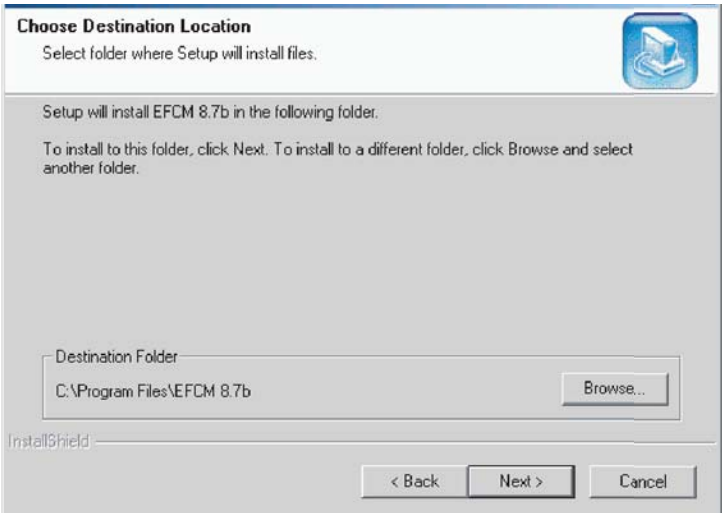

Choose Destination Location
Select folder where Setup will install files.
Setup will install EFCM 8.7b in the following folder.
To install to this folder, click Next. To install to a different folder, click Browse and select another folder.
Destination Folder
C:\Program Files\EFCM 8.7b
Browse...
InstallShield
< Back
Next >
Cancel
6M2027

Figure 66 InstallShield Wizard dialog box

5. Follow the online instructions for the *InstallShield Wizard*. Click *Next* and *Finish* as appropriate.
6. Power off and reboot the server.
   a. *Restart* Windows.

      The server powers down and restarts. During the reboot process, the LAN connection between the server and browser-capable PC drops momentarily, and the TightVNC viewer displays a network error.

   b. After the server reboots, click *Login again*. The *VNC Authentication* screen appears.

   c. Type the default password and click *OK*. The *Welcome to Windows* dialog box appears.

      NOTE: The default TightVNC viewer password is **password.**

   d. Click the **Send Ctrl-Alt-Del** button at the top of the window to log on to the server desktop. The *Log On to Windows* dialog box appears.

NOTE: Do not simultaneously press the **Ctrl**, **Alt**, and **Delete** keys. This action logs the user on to the browser-capable PC, not the rack-mount management server.

e. Type the default Windows user name and password and click *OK*. The server's Windows desktop opens and the *EFCM Log In* dialog box appears.

NOTE: The default Windows user name is **Administrator** and the default password is **password**. Both are case-sensitive.

f. Type the SAN management application default user ID and password and select a server or IP address from the *Network Address* drop-down list.

NOTE: The default SAN management application user ID is **Administrator** and the default password is **password.** Both are case-sensitive.

g. Click *Login*. The application opens and the main window appears.

Chapter 5: Removal and replacement procedures

This chapter describes part removal and replacement procedures (RRPs) for the SAN32M-2 switch. The chapter also provides procedural notes, electrostatic discharge (ESD) precautions, and list of the parts.

NOTE: This section covers both CRUs, customer-replaceable units that are SFPs only, and FRUs (the power supply), field-replaceable units to be replaced only by service personnel.

Procedural notes

Observe the following procedural notes:

1. Follow all ESD precautions and **DANGER**, **CAUTION**, and **ATTENTION** statements.
2. Do not perform an RRP unless a failure is isolated to a part. If fault isolation was not performed, refer to *MAP 0000: Start MAP*.
3. Before removing a part, read the associated RRP to familiarize yourself with the procedure.
4. After completing an RRP:
   - — Clear the event codes reporting the failure and recovery from the product *Event Log*.
   - — Extinguish the amber system error light-emitting diode (LED) at the product front panel.

ESD procedures

Follow these ESD procedures:

- If the product is connected to facility power (grounded), wear an ESD wrist strap and grounding cable connected to the product chassis.
- If the product is not connected to facility power (not grounded), wear an ESD wrist strap and grounding cable connected to an approved bench grounding point.

© Copyright IBM Corp. 2006

- Touch the product chassis once before performing a procedure, and once each minute during the procedure.
- Store ESD-sensitive parts in antistatic packaging.

Customer-replaceable unit: SFP optical transceiver

The small form factor pluggable optical transceiver is a concurrent part that is removed and replaced while the product is powered on and operational.

There are ESD precautions for the part.

Refer to Chapter 6, *Illustrated parts breakdown* for the part locations and part numbers.

Tools required

The following tools are required:

- Protective cap (provided with the fiber-optic jumper cable).
- Loopback plug (provided with the product).
- Fiber-optic cleaning kit.
- ESD grounding cable and wrist strap.

A 5/16-inch door tool may be used for some procedures.

Removal

To remove an SFP optical transceiver:

1. Notify the customer that the port with the defective transceiver will be blocked. Ensure the customer's system administrator sets any attached device offline.
2. If the product is not rack-mounted, go to step 3. If the product is rack-mounted, perform one of the following:
   - — If the product is installed in an equipment cabinet, insert the 5/16-inch door tool into the socket hole at the right top of the door (front or rear). Turn the tool counter- clockwise to unlock and open the door.
   - — If the product is installed in a customer-supplied equipment cabinet, unlock and open the cabinet door (front or rear) as directed by the customer representative.
3. Identify the defective port transceiver from:
   - — An illuminated amber LED adjacent to the port.

— At a web browser communicating with the EFCM Basic Edition interface, port failure information displayed at the *Hardware View*, *Port List View*, or *Event Log*.

— At the management server (Element Manager application), port failure information displayed at the *Hardware View*, *Port List View*, *Port Properties* dialog box, or *Event Log*.

4. Block communication to the port. Refer to *Block or unblock a port* (EFCM Basic Edition) or *Block or unblock a port* (SAN management application) for instructions.
5. Ensure an ESD grounding cable is connected to the product chassis (or approved bench ground) and your wrist.
6. Disconnect the fiber-optic jumper cable from the port:
   a. Pull the keyed LC connector free from the port's optical transceiver.
   b. Place a protective cap over the jumper cable connector.
7. The optical transceiver has a wire locking bale to secure the transceiver in the port receptacle and to assist in removal. The bale rotates up or down, depending on transceiver manufacturer and port location (top or bottom row).
   a. Disengage the locking mechanism by rotating the wire bale up or down 90 degrees as shown in part (1) of Figure 67.
   b. Grasp the wire bale and pull the transceiver from the port receptacle as shown in part (2) of Figure 67.

Figure 67 **SFP optical transceiver removal and replacement**

8. Inspect the *Event Log*:
   - — At a web browser communicating with the EFCM Basic Edition interface, select *Event* from the *Logs* menu.
   - — At the management server (Element Manager application), select *Event Log* from the *Logs* menu.

   An event code **513** (SFP optics hot-removal completed) appears in the *Event Log*.

Replacement

To replace an SFP optical transceiver:

1. Ensure an ESD grounding cable is connected to the product chassis (or approved bench ground) and your wrist.
2. Remove the replacement transceiver from its packaging.

3. Insert the transceiver into the port receptacle, then engage the locking mechanism by rotating the wire bale up or down 90 degrees as shown in Figure 67.
4. Perform an external loopback test. Refer to *External loopback test* (EFCM Basic Edition) or *External loopback test* (SAN management application) for instructions. If the test fails, go to *MAP 0000: Start MAP* to isolate the problem.
5. Reconnect the fiber-optic jumper cable:
   a. Remove the protective cap from the cable connector and the protective plug from the port optical transceiver. Store the cap and plug in a suitable location for safekeeping.
   b. Clean the jumper cable and transceiver connectors. Refer to *Clean fiber-optic components* for instructions.
   c. Insert the keyed LC cable connector into the port's optical transceiver.
6. Ensure the amber port LED extinguishes. If the LED illuminates, go to *MAP 0000: Start MAP* to isolate the problem.
7. Inspect the *Event Log*:
   — At a web browser communicating with the EFCM Basic Edition interface, select *Event* from the *Logs* menu.
   — At the management server (Element Manager application), select *Event Log* from the *Logs* menu.

   Ensure an event code **510** (SFP optics hot-insertion initiated) appears. If the event code does not appear, go to *MAP 0000: Start MAP* to isolate the problem.
8. Verify port operation:
   — At a web browser communicating with the EFCM Basic Edition interface, open the *Hardware View*:
      a. Ensure alert symbols do not appear (yellow triangle or red diamond).
      b. Open the *Port List View*. Verify that port *Operational State*, *Type*, *Health Status*, and *Transceiver* are correct.
   — At the management server (Element Manager application), open the *Hardware View*:

a. Ensure alert symbols do not appear (yellow triangle or red diamond).

b. Double-click the port graphic to open the *Port Properties* dialog box. Verify port information is correct.

c. Right-click the port graphic and select *Port Technology* from the menu. The *Port Technology* dialog box displays. Verify the port technology is correct.

If a problem is indicated, go to *MAP 0000: Start MAP* to isolate the problem.

9. Restore communication to the port as directed by the customer. Refer to *Block or unblock a port* (EFCM Basic Edition) or *Block or unblock a port* (SAN management application) for instructions. Inform the customer the port is available.

10. Clear the system error LED on the product front bezel:

— At a web browser communicating with the EFCM Basic Edition interface, select *Clear System Error Light* from the *Maintenance* menu.

— At the management server (Element Manager application), open the *Hardware View*. Right-click the front panel bezel graphic (away from a FRU/CRU), then click the *Clear System Error Light* menu selection.

11. If necessary, close and lock the equipment cabinet door.

Field-replaceable unit: Redundant power supply

NOTE: These instructions are for service personnel **only**.

The redundant power supply should be replaced by service personnel only.

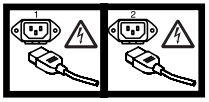
Refer to Chapter 6, *Illustrated parts breakdown* for part locations and part numbers.

Removal

To remove a redundant external power supply:

1. If the product is not rack-mounted, go to step 2. If the product is rack-mounted, unlock and open the cabinet door (front or rear) as directed by the customer representative.

2. Identify the defective power supply from:
   - — Observing that the green LED on the FRU is off.
   - — At a web browser communicating with the EFCM Basic Edition interface or at the management server (Element Manager application), FRU failure information displayed at the *Hardware View*, *FRU List View*, or *Event Log*.
3. Disconnect the AC power cord from facility power.



DANGER

Multiple power cords (L003)

4. Disengage and remove the power supply:
   a. Disengage the locking mechanism by rotating both finger handles outward 90 degrees as shown in part (1) of Figure 68.
   b. Use the finger handles to pull the power supply out of the switch chassis as shown in part (2) of Figure 68. Support the power supply as it is pulled from the chassis.

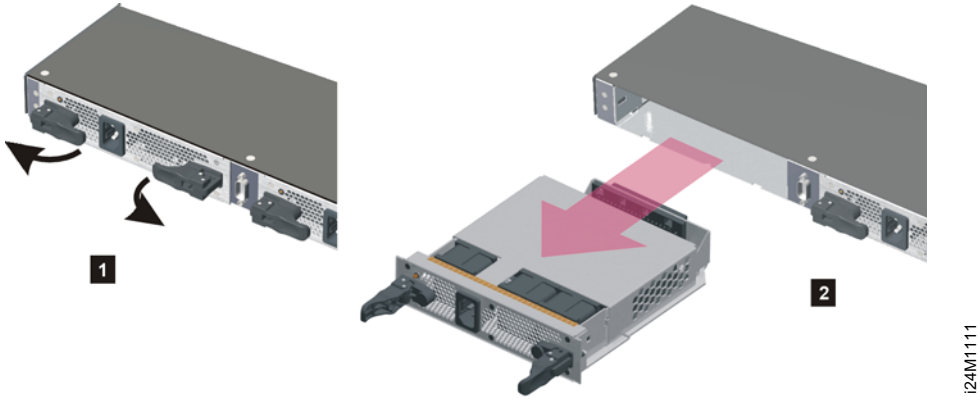


Figure 68 Redundant power supply removal and replacement

5. Inspect the *Event Log*:
   - — At a web browser communicating with the EFCM Basic Edition interface, select *Event* from the *Logs* menu.

— At the management server (Element Manager application), select *Event Log* from the *Logs* menu.

The following event codes appear:

- **200 -** Power supply AC voltage failure (recorded when power is disconnected).
- **206 -** Power supply removed.
- **300 -** Cooling fan propeller failed.

Replacement

To replace a redundant power supply:

1. Remove the replacement power supply from its packaging.
2. Inspect the rear of the power supply for bent or broken connector pins damaged during shipping. If any pins are damaged, obtain a new power supply.
3. Position the power supply in the rear of the switch as shown in part (2) of Figure 68. Ensure the finger handles are disengaged and rotated 90 degrees outward.
   a. While supporting the power supply with one hand, insert it into the switch chassis.
   b. Firmly push the power supply into the chassis. Rotate the finger handles 90 degrees inward to seat the power supply and engage the connector pins. Ensure the faceplate is flush with the chassis cutout.
4. Connect the AC power cord to the power supply and a facility power source.
5. Wait several seconds, then inspect the power supply to ensure the amber LED extinguishes. If the LED illuminates, go to *MAP 0000: Start MAP* to isolate the problem.
6. Inspect the *Event Log*:
   — At a web browser communicating with the EFCM Basic Edition interface, select *Event* from the *Logs* menu.
   — At the management server (Element Manager application), select *Event Log* from the *Logs* menu.

   Ensure the following event codes appear:
   - **203 -** Power supply AC voltage recovery.
   - **207 -** Power supply installed.

- **315 -** Cooling fan propeller recovered.

If the event codes do not appear, go to *MAP 0000: Start MAP* to isolate the problem.

7. Verify power supply operation. At a web browser communicating with the EFCM Basic Edition interface or at the management server (Element Manager application), open the *Hardware View* and observe the FRU graphic to ensure alert symbols do not appear (yellow triangle or red diamond).

   If a problem is indicated, go to *MAP 0000: Start MAP* to isolate the problem.

8. Perform the data collection procedure. Refer to *Collect maintenance data* (EFCM Basic Edition) or *Collect maintenance data* (SAN management application) for instructions.

9. Clear the system error LED on the product front bezel:

   — At a web browser communicating with the EFCM Basic Edition interface, select *Clear System Error Light* from the *Maintenance* menu.

   — At the management server (Element Manager application), open the *Hardware View*. Right-click the front panel bezel graphic (away from a FRU), then click the *Clear System Error Light* menu selection.

10. If necessary, close and lock the equipment cabinet door.

Chapter 6: Illustrated parts breakdown

This chapter provides an illustrated parts breakdown for IBM TotalStorage SAN32M-2 switch customer-replaceable units (CRUs). Exploded-view assembly drawings are provided for:

- Front-accessible CRUs.
- Rear-accessible CRUs.
- Miscellaneous parts.
- Power cords and receptacles.

Exploded-view illustrations portray the switch disassembly sequence for clarity. Illustrated CRUs are numerically keyed to associated tabular part lists. The lists also include part numbers, descriptions, and quantities.

© Copyright IBM Corp. 2006

Front-accessible FRUs

Figure 69 illustrates front-accessible FRUs **(1)**. Contact IBM to order appropriate SFPs.

NOTE: For longwave SFPs, use these part numbers: LW 4 Gpbs, 4 Km use 23R1449; LW 4 Gbps, 10Km use 23R1450, and LW 2 Gpbs, use 19K1281. For shotwave SPFs: use these part numbers: SW 2 Gpbs, 19K1280, and SW 4 Gps, 77P2964. For additional information, contact IBM.

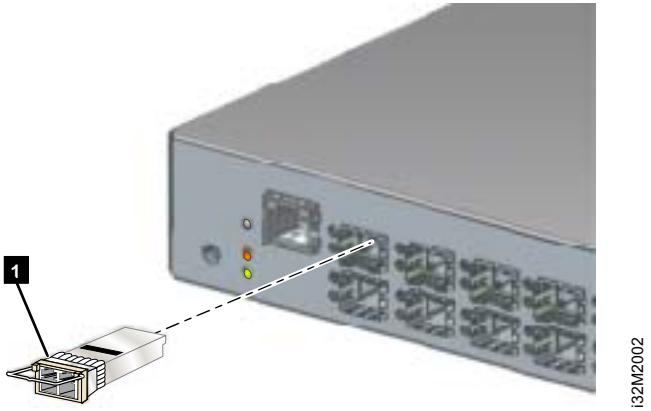


Figure 69 Front-accessible SFPs

Rear-accessible FRUs

Figure 70 illustrates rear-accessible FRUs. Table 30 is the associated FRU parts list. The table includes reference numbers to Figure 70, FRU part numbers, descriptions, and quantities.

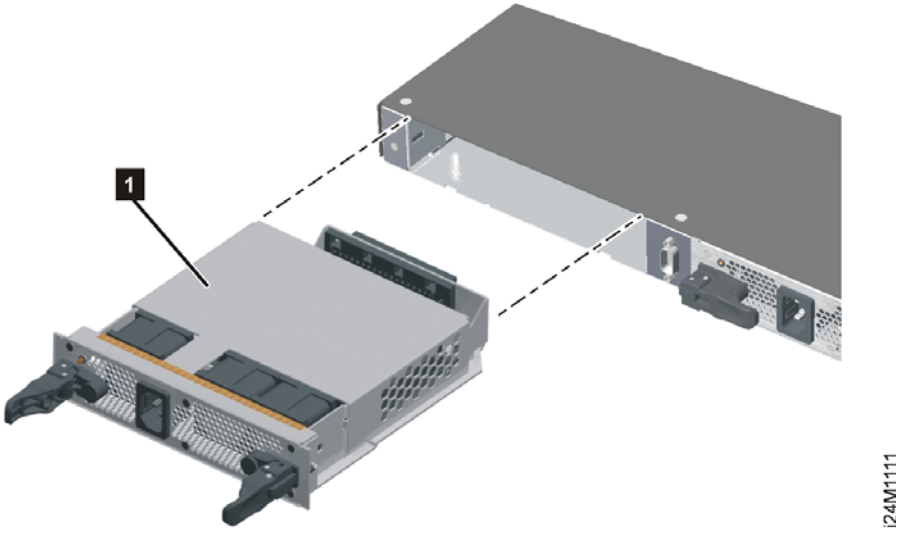


Figure 70 Rear-accessible FRUs

When ordering spare parts, note:

- If the serial number of the switch ends with an alphabetic character, you must install parts with part numbers only from column A.
- For other serial numbers, you can install parts with part numbers from either column A or column B.

Table 30 Rear-accessible FRU parts list

Ref.	Column A	Column B	Description	Qty.
Figure 70	22R5440	23R0706	Switch, SAN32M-2, base assembly	Reference
1	22R5442	23R0707	Power supply assembly, 125-watt rated, 12 VDC output (includes three fan assemblies as part of the CRU)	2

Power cords and receptacles

Figure 71 illustrates optional power cords and receptacles. Table 31 is the associated parts list. The table includes reference numbers to Figure 71, feature numbers, and descriptions.

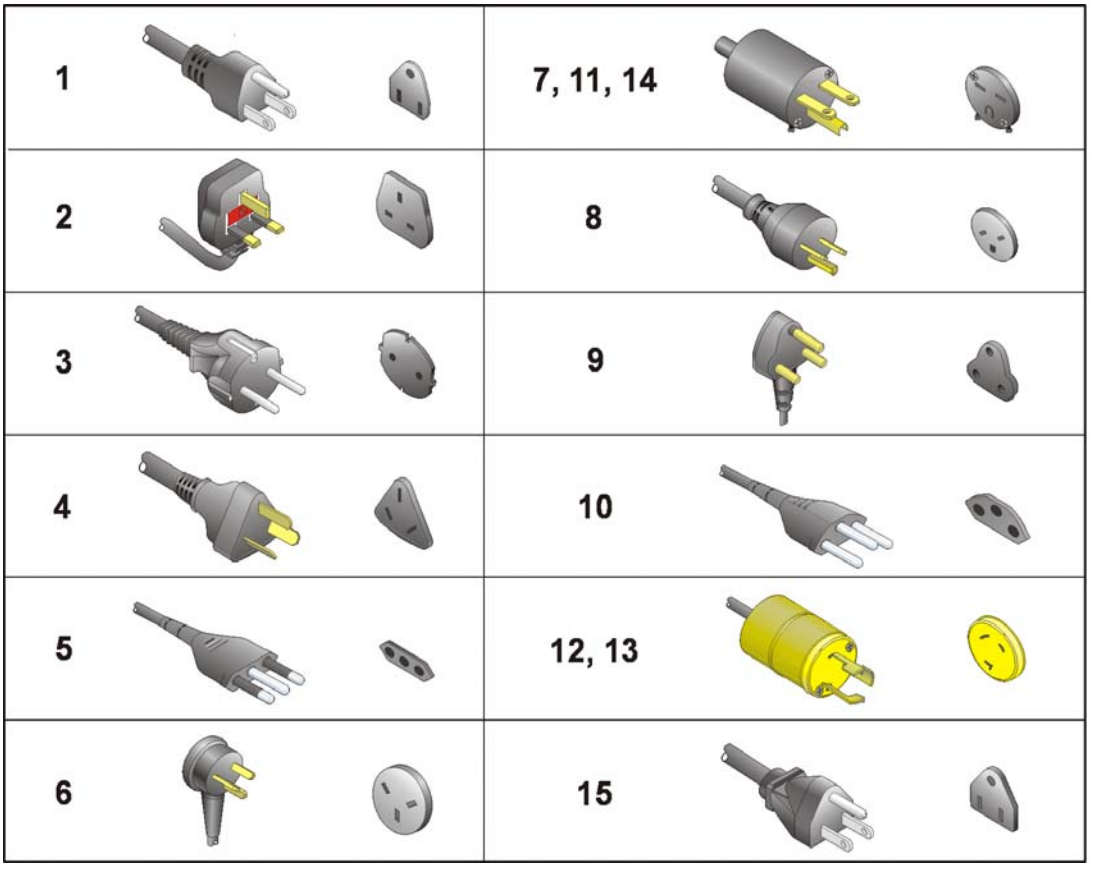


Figure 71 Power cords and receptacles

Table 31 Power cord and receptacle list

Ref.	Part number	Description	Feature
1	Reference only	Power cord, AC, North America NEMA 5-15P straight, 125 volts, 10 amps, 3.0 meters Receptacle: NEMA 5-15R	1010
2	Reference only	Power cord, AC, United Kingdom BS 1363 right angle, 250 volts, 10 amps, 2.8 meters Receptacle: BS 1363	1012
3	Reference only	Power cord, AC, European Union CEE 7/7 straight, 250 volts, 10 amps, 2.8 meters Receptacle: CEE 7	1013
4	Reference only	Power cord, AC, Australia AS 3112 straight, 250 volts, 10 amps, 2.8 meters Receptacle: AS 3112	1014
5	Reference only	Power cord, AC, Italy, Chile, Libya, and Ethiopia CEI 23-16/VII straight, 250 volts, 10 amps, 2.8 meters Receptacle: CEI 23-16/VII	1021
6	Reference only	Power cord, AC, Israel SI-32 right angle, 250 volts, 15 amps, 2.8 meters Receptacle: SI-32	1022
7	Reference only	Power cord, AC, Thailand, Philippines, Taiwan, Bolivia, and Peru NEMA 6-15P straight, 250 volts, 15 amps, 2.8 meters Receptacle: NEMA 6-15R	1023
8	Reference only	Power cord, AC, Denmark Afsnit 107-2-D1 straight, 250 volts, 10 amps, 2.8 meters Receptacle: Afsnit 107-2-D1	1024
9	Reference only	Power cord, AC, South Africa, Burma, Pakistan, India, and Bangladesh BS 546 Type, right angle, 250 volts, 15 amps, 2.8 meters Receptacle: BS 546	1025
10	Reference only	Power cord, AC, Switzerland and Liechtenstein SEV 1011 straight, 250 volts, 10 amps, 2.8 meters Receptacle: SEV 1011	1026
11	Reference only	Power cord, AC, United States (Chicago) NEMA 6-15P straight, non-locking, 250 volts, 10 amps, 1.8 meters Receptacle: NEMA 6-15R	1027

Table 31 Power cord and receptacle list (Continued)

Ref.	Part number	Description	Feature
12	Reference only	Power cord, AC, United States (Chicago) NEMA L6-15P straight, twist-lock, 250 volts, 10 amps, 1.8 meters Receptacle: NEMA L6-15R	1028
13	Reference only	Power cord, AC, North America NEMA L6-15P straight, twist-lock, 250 volts, 10 amps, 2.8 meters Receptacle: NEMA L6-15R	1016 and 1029
14	Reference only	Power cord, AC, Japan NEMA 6-15P straight, 240 volts, 6 amps, 2.8 meters Receptacle: NEMA 6-15R **Note:** The power cord shipped is specifically intended for use with the associated product and cannot be used with any other electrical products.	1030
15	Reference only	Power cord, AC, Japan JIS 8303 straight, 125 volts, 12 amps, 2.5 meters Receptacle: NEMA 5-15R **Note:** The power cord shipped is specifically intended for use with the associated product and cannot be used with any other electrical products.	None

Appendix A: Event code tables

An event is a state change, problem detection, or problem correction that requires attention or should be reported to service personnel. An event usually indicates an operational state transition, but may also indicate an impending state change (threshold violation) or provide information only. Events are reported as event codes. This appendix lists three-digit event codes. The codes are listed in numerical order and tabular format as follows:

- **000** through **199** - system events.
- **200** through **299** - power supply events.
- **300** through **399** - fan events.
- **400** through **499** - control processor (CTP) card events.
- **500** through **599** - port events.
- **800** through **899** - thermal sensor events.

Events are recorded in the *Event Log* at the Enterprise Fabric Connectivity Manager (EFCM) Basic Edition interface or rack-mount management server (Element Manager application). An event illuminates the system error light-emitting diode (LED) at the product front panel.

Tables in this appendix also provide a:

- **Message -** a text string that describes the event.
- **Severity -** a severity level that indicates event criticality as follows:
  - **0 -** informational.
  - **2 -** minor.
  - **3 -** major.
  - **4 -** severe (not operational).
- **Explanation -** an explanation of what caused the event.
- **Action -** the recommended action (if any) to resolve the problem.
- **Event data -** supplementary event data (if any) that appears in the event log in hexadecimal format.

© Copyright IBM Corp. 2006

- **Distribution -** checks in associated fields indicate where the event code is reported (product, management server, or attached host).

System events (000 through 199)

Event Code: 001							
Message:	System power-down.						
Severity:	Informational.						
Explanation:	The director was powered off or disconnected from the facility AC power source. The event code is distributed the next time the director powers on, but the date and time of the code reflect the power-off time.						
Action:	No action required.						
Event Data:	No supplementary data included with the event.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✔		✔				

Event code: 011							
Message:	Login Server database invalid.						
Severity:	Minor.						
Explanation:	Following an initial machine load (IML) or firmware download, the Login Server database failed cyclic redundancy check (CRC) validation. All fabric service databases initialize to an empty state, resulting in implicit fabric logout of all attached devices.						
Action:	Perform a data collection and return the CD to support personnel.						
Event data:	No supplementary data included.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔	✔	✔	✔	✔		

Event code: 021							
Message:	Name Server database invalid.						
Severity:	Minor.						
Explanation:	Following an IML or firmware download, the Name Server database failed CRC validation. All fabric service databases initialize to an empty state, resulting in implicit fabric logout of all attached devices.						
Action:	Perform a data collection and return the CD to support personnel.						
Event data:	No supplementary data included.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔	✔	✔	✔	✔		

Event code: 031							
Message:	SNMP request received from unauthorized community.						
Severity:	Informational.						
Explanation:	An SNMP request containing an unauthorized community name was rejected with an error. Only requests containing authorized SNMP community names configured through the Element Manager application are allowed.						
Action:	Add the community name to the SNMP configuration using the Element Manager application.						
Event data:	No supplementary data included.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Event code: 051							
Message:	Management Server database invalid.						
Severity:	Minor.						
Explanation:	Following an IML or firmware download, the Management Server database failed CRC validation. All management service databases initialize to an empty state, resulting in implicit logout of all logged-in devices.						
Action:	Perform a data collection and return the CD to support personnel.						
Event data:	No supplementary data included.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔	✔	✔	✔	✔		

Event Code: 052							
Message:	Management Server internal error.						
Severity:	Informational.						
Explanation:	An internal operating error was detected by the management server application.						
Action:	Management server application internal error: Perform the data collection procedure and return the CD to support personnel.						
Event Data:	Supplementary data consists of reporting tasks of type **eMST_SB2**, with component_id **eMSCID_SB2_CHPGM**. For each type of error or indication, the subcomponent_id is: Management server internal error: subcomponent_id is **eMS_ELR_SB2_DEVICE_PROTOCOL_ERROR** or **eMS_ELR_SB2_MSG_PROCESSING_ERROR**.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✔		✔			✔	

Event code: 061							
Message:	Fabric Controller database invalid.						
Severity:	Minor.						
Explanation:	Following an IML or firmware download, the fabric controller database failed CRC validation. All fabric controller databases initialize to an empty state, resulting in momentary loss of interswitch communication.						
Action:	Perform a data collection and return the CD to support personnel.						
Event data:	No supplementary data included.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔	✔	✔	✔	✔		

Event code: 062							
Message:	Maximum interswitch hop count exceeded.						
Severity:	Informational.						
Explanation:	Fabric controller software detected a path to a director or switch that traverses more than seven interswitch links (hops). This may result in Fibre Channel frames persisting in the fabric longer than timeout values allow.						
Action:	Reconfigure the fabric so the path between any two switches traverses seven or less ISLs.						
Event data:	Byte **0** = domain ID of the director or switch more than seven hops away.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Event code: 063							
Message:	Remote switch has too many ISLs.						
Severity:	Major.						
Explanation:	The director or switch with domain ID indicated in the event data has too many ISLs attached and is unreachable from this switch. SAN management application Version 3.2 and earlier supports up to 32 ISLs. SAN management application Version 3.3 and later supports up to 128 ISLs.						
Action:	Reduce the ISLs on the indicated director or switch to a number within limits specified.						
Event data:	Byte **0** = domain ID of the director or switch with too many ISLs.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔	✔	✔	✔			

Event code: 064							
Message:	ESS response from indicated domain ID not received after maximum tries.						
Severity:	Informational.						
Explanation:	Fabric controller software detected an exchange switch support (ESS) response from the indicated domain ID was not received after the maximum attempts. The event is reported only in McDATA interop mode.						
Action:	None.						
Event data:	Byte **0** = domain ID of the director or switch not receiving an ESS response. Byte **1** = domain ID of the director or switch not responding.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

<table>
<tr><th colspan="8">Event code: 070</th></tr>
<tr><td>Message:</td><td colspan="7">E_Port is segmented.</td></tr>
<tr><td>Severity:</td><td colspan="7">Informational.</td></tr>
<tr><td>Explanation:</td><td colspan="7">An E_Port recognized an incompatibility with the attached director or switch, preventing fabric participation. A segmented port does not transmit Class 2 or Class 3 traffic, but transmits Class F traffic. Refer to event data for segmentation reason.</td></tr>
<tr><td>Action:</td><td colspan="7">Action depends on segmentation reason specified.</td></tr>
<tr><td>Event data:</td><td colspan="7">The first byte of event data (byte 0) specifies the E_Port number. The fifth byte (byte 4) specifies the segmentation reason as follows:

1 = Incompatible operating parameters - Ether the resource allocation time out value (R_A_TOV) or error detect time out value (E_D_TOV) is inconsistent between the switch and another director or switch. Modify the R_A_TOV and E_D_TOV to make the values consistent.

2 = Duplicate domain ID - The switch has the same preferred domain ID as another director or switch) Modify the Domain ID to make it unique.

3 = Incompatible zoning configurations - The same name is applied to a zone for the switch and another director or switch, but the zones contain different zone members. Modify the zone name to make it unique, or ensure zones with the same name contain identical zone members.

4 = Build fabric protocol error - A protocol error was detected during incorporation of the switch into the fabric. Disconnect the E_Port link, then reconnect the link. If the condition persists, perform a data collection and return the CD to support personnel.

5 = No principal switch - No director or switch in the fabric can become the principal switch. Modify the switch priority to any value other than 255.

6 = No response from attached switch (hello timeout) - The switch periodically verifies operation of attached directors or switches. The E_Port at the operational switch times out and segments if the attached device does not respond. Check the status of the attached director or switch. If the condition persists, perform a data collection and return the CD to support personnel.</td></tr>
<tr><td rowspan="3">Distribution:</td><td colspan="2">Product</td><td colspan="3">Management Server</td><td colspan="2">Host</td></tr>
<tr><td>EFCM Basic Event Log</td><td>System Error LED</td><td>Event Log</td><td>E-Mail</td><td>Call-Home</td><td>Sense Info</td><td>Link Incident Log</td></tr>
<tr><td>✔</td><td></td><td>✔</td><td>✔</td><td></td><td></td><td></td></tr>
</table>

<table>
<tr><th colspan="8">Event code: 071</th></tr>
<tr><td>Message:</td><td colspan="7">Switch is isolated.</td></tr>
<tr><td>Severity:</td><td colspan="7">Informational.</td></tr>
<tr><td>Explanation:</td><td colspan="7">The switch is isolated from other directors or switches. This event code is accompanied by one or more 070 event codes. Refer to event data for segmentation reason.</td></tr>
<tr><td>Action:</td><td colspan="7">Action depends on segmentation reason specified.</td></tr>
<tr><td>Event data:</td><td colspan="7">The first byte of event data (byte 0) specifies the E_Port number. The fifth byte (byte 4) specifies the segmentation reason as follows:

1 = Incompatible operating parameters - Ether the resource allocation time out value (R_A_TOV) or error detect time out value (E_D_TOV) is inconsistent between the switch and another director or switch. Modify the R_A_TOV and E_D_TOV to make the values consistent.

2 = Duplicate domain ID - The switch has the same preferred domain ID as another director or switch) Modify the Domain ID to make it unique.

3 = Incompatible zoning configurations - The same name is applied to a zone for the switch and another director or switch, but the zones contain different zone members. Modify the zone name to make it unique, or ensure zones with the same name contain identical zone members.

4 = Build fabric protocol error - A protocol error was detected during incorporation of the switch into the fabric. Disconnect the E_Port link, then reconnect the link. If the condition persists, perform a data collection and return the CD to support personnel.

5 = No principal switch - No director or switch in the fabric can become the principal switch. Modify the switch priority to any value other than 255.

6 = No response from attached switch (hello timeout) - The switch periodically verifies operation of attached directors or switches. The E_Port at the operational switch times out and segments if the attached device does not respond. Check the status of the attached director or switch. If the condition persists, perform a data collection and return the CD to support personnel.</td></tr>
<tr><td rowspan="3">Distribution:</td><td colspan="2">Product</td><td colspan="3">Management Server</td><td colspan="2">Host</td></tr>
<tr><td>EFCM Basic Event Log</td><td>System Error LED</td><td>Event Log</td><td>E-Mail</td><td>Call-Home</td><td>Sense Info</td><td>Link Incident Log</td></tr>
<tr><td>✔</td><td></td><td>✔</td><td></td><td></td><td></td><td></td></tr>
</table>

Event code: 072							
Message:	E_Port connected to unsupported switch.						
Severity:	Informational.						
Explanation:	The switch is attached (through an ISL) to an incompatible director or switch.						
Action:	Disconnect the ISL.						
Event data:	No supplementary data included.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Event code: 073							
Message:	Fabric initialization error.						
Severity:	Informational.						
Explanation:	An error was detected during the fabric initialization sequence, probably caused by frame delivery errors. Event data is intended for engineering evaluation.						
Action:	Perform a data collection and return the CD to support personnel.						
Event data:	Byte **0** = error reason code for engineering evaluation. Bytes **4** - **9** = port numbers where problems were detected.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Event code: 074							
Message:	ILS frame delivery error threshold exceeded.						
Severity:	Informational.						
Explanation:	Fabric controller frame delivery errors exceeded an E_Port threshold and caused fabric initialization problems (**073** event code). Most problems are caused by control frame delivery errors, as indicated by this code. Event data is intended for engineering evaluation.						
Action:	Perform a data collection and return the CD to support personnel.						
Event data:	Byte **0** = E_Port number reporting the problem. Bytes **4** - **8** = Count of frame delivery timeouts. Bytes **9** - **11** = Count of frame delivery aborts.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Event code: 075							
Message:	E_Port segmentation recovery.						
Severity:	Informational.						
Explanation:	A segmented E_Port (event code **070**) recovered. This event is not generated if the port is manually recovered by blocking and unblocking, setting offline and online, or disconnecting the fiber-optic cable.						
Action:	None.						
Event data:	The first byte of event data (byte **0**) specifies the E_Port number. The fifth byte (byte **4**) specifies the original segmentation reason as described in event code **070**.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔	✔			

Event Code: 076							
Message:	Out of Range Domain ID detected.						
Severity:	Informational.						
Explanation:	Switch has detected a domain ID that is out of the supported range behind the attached ISL. This event may be followed by a segmentation event 070.						
Action:	Check that all McDATA switches in the fabric are configured with the same domain id offset. Check that all non-McDATA switches are configured with a domain id that is within the range of this switch (offset + 1 ' offset + 31). .						
Event Data:	<See subsequent tables> ALL DATA IS BIG ENDIAN						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✔		✔	✔			

Event code: 080							
Message:	Unauthorized worldwide name.						
Severity:	Informational.						
Explanation:	The WWN of the connected device or fabric element is not authorized for the port number.						
Action:	Change the port binding definition or connect the proper device or fabric element to the indicated port.						
Event data:	Byte **0** = Port number reporting the unauthorized connection. Bytes **4** - **11** = WWN of the unauthorized device or fabric element.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔	✔			

Event code: 081	
Message:	Invalid attachment.
Severity:	Informational.
Explanation:	A switch port recognized an incompatibility with the attached fabric element or device and isolated the port. An isolated port does not transmit Class 2, Class 3, or Class F traffic. Refer to event data for the reason.
Action:	Action depends on reason specified.
Event data:	The first byte of event data (byte **0**) specifies the port number. The fifth byte (byte **4**) specifies the isolation reason as follows: **1 = Unknown -** Reason is unknown, but probably caused by failure of an E_Port connected device. Fault isolate the failed device or contact support personnel to report the problem. **2 = ISL connection not allowed -** The port connection conflicts with the configured port type. Change the port type to **F_Port** if the port is cabled to a device, or **E_Port** if the port is cabled to a fabric element to form an ISL. **3 = Incompatible switch -** The switch returned a *Process ELP Reject - Unable to Process* reason code because the attached fabric element is not compatible. Set the switch operating mode to **McDATA Fabric 1.0** if connected to an IBM product. Set the switch operating mode to **Open Fabric 1.0** if connected to an open-fabric compliant product manufactured by a different vendor. **4 = Incompatible switch -** The switch returned a *Process ELP Reject - Invalid Revision Level* reason code because the attached fabric element is not compatible. Set the switch operating mode to **McDATA Fabric 1.0** if connected to an IBM product. Set the switch operating mode to **Open Fabric 1.0** if connected to an open-fabric compliant product manufactured by a different vendor. **5 = Loopback plug connected -** A loopback plug is connected to the port with no diagnostic test running. Remove the loopback plug. **6 = N_Port connection not allowed -** The switch is connected to a fabric element through a misconfigured port. Change the port type to **E_Port**. **7 = Non-IBM switch at other end -** The attached fabric element is not an IBM product. Set the switch operating mode to **Open Fabric 1.0** if connected to an open-fabric compliant product manufactured by a different vendor. **8 = E_Port capability disabled -** The product does not have E_Port capability. Enable this functionality through the appropriate product feature enablement (PFE) key. **A = Unauthorized port binding WWN -** The device WWN or nickname used to configure port binding for this port is not valid. At the *Configure Ports* dialog box, reconfigure the port with the WWN or nickname authorized for the attached device, or disable the port binding feature.

<table>
<tr><th colspan="8">Event code: 081 (continued)</th></tr>
<tr><td>Event Data (continued):</td><td colspan="7">B = Unresponsive node - The attached node did not respond, resulting in a G_Port ELP timeout. Check the status of the attached device and clean the link's fiber-optic components (cable and connectors). If the problem persists, contact support personnel to report the problem.

C = ESA security mismatch - Processing of the Exchange Security Attribute (ESA) frame detected a security feature mismatch. The switch binding parameters for this switch and the attached fabric element must agree. At the Switch Binding - State Change dialog boxes, ensure the parameters for both fabric elements are compatible, or disable the fabric and switch binding features.

D = Fabric binding mismatch - Fabric binding is enabled and an attached fabric element has an incompatible fabric membership list. At the Fabric Binding dialog box, update the fabric membership list for both fabric elements to ensure compatibility, or disable the fabric binding feature.

E = Authorization failure reject - The fabric element connected to the switch through an ISL detected a security violation. As a result, the switch received a generic reason code and set the port to an invalid attachment state. Check the port status of the attached fabric element and clean the link's fiber-optic components (cable and connectors). If the problem persists, contact support personnel to report the problem.

F = Unauthorized switch binding WWN - Switch binding is enabled and an attached device or fabric element has an incompatible switch membership list. At the Switch Binding - Membership List dialog box, update the switch membership list for the switch and the attached device or fabric element to ensure compatibility, or disable the switch binding feature.

10 = Authentication failure - An ISL challenge handshake authentication protocol (CHAP) check failed. Update the authentication list or disable the authentication feature.

11 = Fabric mode mismatch - Based on the ELP revision level, a connection was not allowed because an IBM switch in legacy mode is attached to an IBM switch in Open Fabric mode, or an IBM switch in Open Fabric mode is attached to an OEM switch at an incorrect ELP revision level. Update the fabric mode for one switch using the Interop Mode drop-down list at the Configure Fabric Parameters dialog box.

12 = CNT WAN extension mode mismatch - Based on switch-to-switch differences between the ELP maximum frame sizes allowed, a connection was not allowed to a switch set to Computer Network Technologies (CNT) wide area network (WAN) extension mode. Contact support personnel to obtain software maintenance release 4.02.00. This release is required to correct the problem and allow switches to communicate with CNT UltraEdge WAN Gateways.</td></tr>
<tr><td rowspan="2">Distribution:</td><td colspan="2">Product</td><td colspan="3">Management Server</td><td colspan="2">Host</td></tr>
<tr><td>EFCM Basic Event Log</td><td>System Error LED</td><td>Event Log</td><td>E-Mail</td><td>Call-Home</td><td>Sense Info</td><td>Link Incident Log</td></tr>
<tr><td></td><td>✔</td><td></td><td>✔</td><td></td><td></td><td>✔</td><td></td></tr>
</table>

Event code: 082							
Message:	Port fenced.						
Severity:	Informational.						
Explanation:	The port was blocked after exceeding threshold criteria defined by the port fencing policy. A hardware malfunction is indicated or the port fencing policy is too restrictive. The fence type is indicated in the event data.						
Action:	Identify and correct the hardware malfunction (port transceiver, fiber-optic cable, or attached fabric element), or change the port fencing threshold settings to more lenient values. After problem correction, unblock the port.						
Event data:	The first byte of event data (byte **0**) specifies the port number. The fifth byte (byte **4**) specifies the fence type code as follows: **1 = Protocol error -** Failure is associated with persistent incomplete operations or application-layer protocol errors (including port logins, fabric rebuilds, and management protocol errors). **2 = Link level hot I/O -** Failure is hardware related and associated with an unstable link-state machine. **3 = Security violation -** Failure is associated with persistent firmware-related security feature violations (port binding violations or authentication failures). The ninth byte (byte **8**) specifies the disabled reason code as follows: **1 = Unknown -** The failure reason is unknown. **9 = ISL fencing -** The E_Port (ISL) was fenced after the port exceeded a threshold value.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔			✔	

Event code: 083	
Message:	Port set to inactive state.
Severity:	Informational.
Explanation:	A hardware or software problem prevented the port from coming online and set the port to an inactive state. Refer to event data for the inactive reason
Action:	Action depends on inactive reason specified.

Event data:	The first byte of event data (byte **0**) specifies the port number. The second byte (byte **1**) specifies the inactive reason code as follows: **2 = Feature key not enabled -** The optional flexport PFE key is not enabled. **3 = Switch speed conflict -** The port cannot operated at the configured product (backplane or CTP Card) speed. **4 = Optics speed conflict -** The port transceiver does not support the configured port speed. **5 = No SBAR -** A serial crossbar (SBAR) is not installed. Not applicable to IBM 2026 type switches. **6 = Port swap conflict -** The port swap configuration is invalid.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔			✔	

Event Code: 084						
Message:	Continuous Incident Detection and Reporting - threshold was exceeded for the port					
Severity:	Informational					
Explanation:	CIDR threshold value exceeded for one of the following incidents • "Unroutable Frames Incident - Port has received unroutable frames • "Routable Good Frames Incident - Port has received frames with embedded port as destination • "Invalid Transmission words Incident - Port has received invalid transmission words The CIDR reason code is indicated in the event data.					
Action:	Helps in identifying the misbehaving device, so that it could be corrected/fixed.					
Event Data:	See Event #84 Data table below					
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✔		✔				

Event #84 Data				
	Byte 0	Byte 1	Byte 2	Byte 3
Word 0	Port Number			
Word 1	CIDR Reason Code (See Event #84 CIDR Event Reason Code table below)			
Word 2	CIDR Event Type (See Event #84 CIDR Event Type table below)			

Event #84 CIDR Reason Code		
Code	**Type**	**Description**
0xFF01	Unroutable Frames Incident	Port has received unroutable frames
0xFF02	Good Frames Incident	Port has received frames with embedded port as destination
0xFF03	Invalid Transmission Words Incident	Port has received invalid transmission words
Event #84 CIDR Event Type		
Code	**Type**	**Description**
0x01	Short Event	Incident was repeated several times in the past five minutes.
0x02	MediumEvent	Incident was repeated several times in the past one hour.
0x03	LongEvent	Incident was repeated several times in the past 24 hours.

Event Code: 085							
Message:	Continuous Incident Detection and Reporting with E-Mail - CIDR threshold was exceeded for the port and this event will trigger an E-Mail.						
Severity:	Informational.						
Explanation:	CIDR threshold value exceeded for one of the following incidents • Unroutable Frames Incident - Port continuously receiving unroutable frames • Routable Good Frames Incident - Port continuously receiving frames with embedded port as destination • "Invalid Transmission words Incident - Port continuously receiving frames with invalid transmission words The CIDR reason code is indicated in the event data.						
Action:	Identify the responsible device and fix.						
Event Data:	See Event #84 Data table.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✔		✔	✔			

Event Code: 086							
Message:	Continuous Incident Detection and Reporting with Call Home - CIDR threshold was exceeded for the port and this event will trigger E-Mail as well as Call Home.						
Severity:	Informational.						
Explanation:	CIDR threshold value exceeded for one of the following incidents • Unroutable Frames Incident - Port continuously receiving unroutable frames • Routable Good Frames Incident - Port continuously receiving frames with embedded port as destination • Invalid Transmission words Incident - Port continuously receiving frames with invalid transmission words The CIDR reason code is indicated in the event data.						
Action:	Identify the responsible device and fix.						
Event Data:	See Event #84 Data table.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✔		✔	✔	✔		

Event code: 120							
Message:	Error detected while processing system management command.						
Severity:	Informational.						
Explanation:	This event occurs when the switch receives a management command that violates specified boundary conditions, typically as a result of a network error. The switch rejects the command, drops the switch-to-server Ethernet link, and forces error recovery processing. When the link recovers, the command can be retried.						
Action:	No action is required for an isolated event. If this event persists, perform a data collection and return the CD to support personnel.						
Event data:	No supplementary data included.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Event code: 121							
Message:	Zone set activation failed - zone set too large.						
Severity:	Informational.						
Explanation:	This event occurs when the switch receives a zone set activation command that exceeds the size supported by the switch. The switch rejects the command, drops the switch-to-server Ethernet link, and forces error recovery processing. When the link recovers, the command can be modified and retried.						
Action:	Reduce the size of the zone set to conform to the limit specified, then retry the activation command.						
Event data:	No supplementary data included.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Event code: 140							
Message:	Congestion detected on an ISL.						
Severity:	Informational.						
Explanation:	OpenTrunking firmware detected an ISL with Fibre Channel traffic that exceeded the configured congestion threshold.						
Action:	No action is required for an isolated event. If this event persists, relieve the congestion by adding parallel ISLs, increasing the ISL link speed, or moving device connections to a less-congested region of the fabric.						
Event data:	Byte **0** = Port number reporting congestion.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Event code: 141							
Message:	Congestion relieved on an ISL.						
Severity:	Informational.						
Explanation:	OpenTrunking firmware detected an ISL with Fibre Channel traffic that previously exceeded the configured congestion threshold. The congestion is now relieved.						
Action:	No action required.						
Event data:	Byte **0** = Port number reporting congestion relieved.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Event code: 142							
Message:	Low BB_Credit detected on an ISL.						
Severity:	Informational.						
Explanation:	OpenTrunking firmware detected an ISL with no transmission BB_Credit for a period of time that exceeded the configured low BB_Credit threshold. This indicates downstream fabric congestion.						
Action:	No action is required for an isolated event or if the reporting ISL approaches 100% throughput. If this event persists, relieve the low BB_Credit condition by adding parallel ISLs, increasing the ISL link speed, or moving device connections to a less-congested region of the fabric.						
Event data:	Byte **0** = Port number reporting low BB_Credit.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Event code: 143							
Message:	Low BB_Credit relieved on an ISL.						
Severity:	Informational.						
Explanation:	OpenTrunking firmware detected an ISL with no transmission BB_Credit for a period of time that previously exceeded the configured low BB_Credit threshold. The low-credit condition is now relieved.						
Action:	No action required.						
Event data:	Byte **0** = Port number reporting low BB_Credit relieved.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Event code: 150							
Message:	Fabric merge failure.						
Severity:	Informational.						
Explanation:	During ISL initialization, the fabric merge process failed. The fabric binding membership lists do not match, an incompatible zone set was detected, there is a problem with exchanging zoning parameters, or the zone set merge failed. This event code is always preceded by a **070** ISL segmentation event code, and represents the reply of an adjacent fabric element. Refer to the event data for the failure reason.						
Action:	Perform a data collection and return the CD to support personnel.						
Event data:	Event data are mapped from the software implementation of the FC-SW2 protocol and are typically complicated. Decoding the event data requires engineering support. Event data are as follows: Bytes **0 - 3** = Affected E_Port number(s). Bytes **4 - 7** = Request SW_ILS command codes. Bytes **8** - **31** = Request response payloads.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔	✔	✔				

<table>
<tr><th colspan="8">Event code: 151</th></tr>
<tr><td>Message:</td><td colspan="7">Fabric configuration failure.</td></tr>
<tr><td>Severity:</td><td colspan="7">Informational.</td></tr>
<tr><td>Explanation:</td><td colspan="7">A fabric-wide configuration activation process failed. An event code 151 is recorded only by the managing switch in the fabric. The event code is intended to help engineering support personnel fault isolate a fabric-wide configuration failures.</td></tr>
<tr><td>Action:</td><td colspan="7">Perform a data collection and return the CD to support personnel.</td></tr>
<tr><td>Event data:</td><td colspan="7">Event data are mapped from the software implementation of the FC-SW2 protocol and are typically complicated. Decoding the event data requires engineering support. Event data are as follows:

Bytes 0 - 3 = Managing switch domain ID in internal format (1-31).
Bytes 4 - 7 = Fabric configuration operation that failed.
Bytes 8 - 11 = Fabric configuration step that failed.
Bytes 12 - 15 = Managed switch domain ID in internal format (1-31).
Bytes 16 - 19 = Response command code received from the managed switch.
Bytes 20 - 23 = Response code received from the managed switch.
Bytes 24 - 27 = Reason code received from the managed switch.
Bytes 28 - 31 = Error code received from the managed switch.</td></tr>
<tr><td rowspan="3">Distribution:</td><td colspan="2">Product</td><td colspan="3">Management Server</td><td colspan="2">Host</td></tr>
<tr><td>EFCM Basic Event Log</td><td>System Error LED</td><td>Event Log</td><td>E-Mail</td><td>Call-Home</td><td>Sense Info</td><td>Link Incident Log</td></tr>
<tr><td>✔</td><td>✔</td><td>✔</td><td></td><td></td><td></td><td></td></tr>
</table>

Power supply events (200 through 299)

Event code: 200							
Message:	Power supply AC voltage failure.						
Severity:	Major.						
Explanation:	AC input to the power supply is disconnected or AC circuitry in the power supply failed. The event only occurs when two power supplies are installed. The second power supply assumes the full operating load.						
Action:	Ensure the power supply is connected to facility AC power and verify operation of the facility power source. If the AC voltage does not recover (indicated by event code **203**), contact IBM to replace the failed power supply. Perform a data collection and return the CD and failed power supply to support personnel.						
Event data:	No supplementary data included.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔	✔	✔	✔	✔	✔	

Event code: 201							
Message:	Power supply DC voltage failure.						
Severity:	Major.						
Explanation:	DC circuitry in the power supply failed. The event only occurs when two power supplies are installed. The second power supply assumes the full operating load.						
Action:	Contact IBM to replace the failed power supply. Perform a data collection and return the CD and failed power supply to support personnel.						
Event data:	No supplementary data included.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔	✔	✔	✔	✔	✔	

Event Code: 202							
Message:	Power supply thermal failure.						
Severity:	Major.						
Explanation:	The thermal sensor associated with a power supply indicates an overheat condition that shut down the power supply. The second power supply assumes the full operating load for the director.						
Action:	Replace the failed power supply. Perform the data collection procedure and return the CD and failed power supply to support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Event code: 203							
Message:	Power supply AC voltage recovery.						
Severity:	Informational.						
Explanation:	AC voltage recovered for the power supply. Both power supplies adjust to share operating load.						
Action:	No action required.						
Event data:	No supplementary data included.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Event code: 204							
Message:	Power supply DC voltage recovery.						
Severity:	Informational.						
Explanation:	DC voltage recovered for the power supply. Both power supplies adjust to share operating load.						
Action:	No action required.						
Event data:	No supplementary data included.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Event code: 206							
Message:	Power supply removed.						
Severity:	Informational.						
Explanation:	A power supply was removed while the switch was powered on and operational. The second power supply assumes the full operating load.						
Action:	No action required or install an operational power supply.						
Event data:	No supplementary data included.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Event code: 207							
Message:	Power supply installed.						
Severity:	Informational.						
Explanation:	A redundant power supply was installed with the switch powered on and operational. Both power supplies adjust to share operating load.						
Action:	No action required.						
Event data:	No supplementary data included.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Event Code: 208							
Message:	Power supply false shutdown.						
Severity:	Major.						
Explanation:	Director operational firmware nearly shut down the indicated power supply as a result of failure or facility power loss or voltage fluctuation.						
Action:	Confirm operation of facility power. If subsequent power loss events occur, replace the failed power supply. Perform the data collection procedure and return the CD and failed power supply to support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Fan events (300 through 399)

Event code: 300							
Message:	Cooling fan propeller failed.						
Severity:	Major.						
Explanation:	One cooling fan failed or is rotating at insufficient angular velocity.						
Action:	Contact IBm to replace the power supply containing the indicated fan module.						
Event data:	The first byte of event data (byte **0**) specifies the failed fan number.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔	✔	✔	✔	✔	✔	

Event code: 301							
Message:	Cooling fan propeller failed.						
Severity:	Major.						
Explanation:	Two cooling fans failed or are rotating at insufficient angular velocity.						
Action:	Contact IBm to replace the power supply containing the indicated fan module.						
Event data:	The first byte of event data (byte **0**) specifies the failed fan number(s).						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔	✔	✔	✔	✔	✔	

Event code: 302	
Message:	Cooling fan propeller failed.
Severity:	Major.

Explanation:	Three cooling fans failed or are rotating at insufficient angular velocity.						
Action:	Contact IBm to replace the power supply containing the indicated fan module.						
Event data:	The first byte of event data (byte **0**) specifies the failed fan number(s).						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔	✔	✔	✔	✔	✔	

Event code: 303							
Message:	Cooling fan propeller failed.						
Severity:	Major.						
Explanation:	Four cooling fans failed or are rotating at insufficient angular velocity.						
Action:	Contact IBm to replace the power supply containing the indicated fan module.						
Event data:	The first byte of event data (byte **0**) specifies the failed fan number(s).						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔	✔	✔	✔	✔	✔	

Event code: 304	
Message:	Cooling fan propeller failed.
Severity:	Major.
Explanation:	Five cooling fans failed or are rotating at insufficient angular velocity.
Action:	Contact IBM to replace both power supplies.
Event data:	The first byte of event data (byte **0**) specifies the failed fan number(s).

Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔	✔	✔	✔	✔	✔	

Event code: 305							
Message:	Cooling fan propeller failed.						
Severity:	Major.						
Explanation:	Six cooling fans failed or are rotating at insufficient angular velocity.						
Action:	Contact IBM to replace both power supplies.						
Event data:	The first byte of event data (byte **0**) specifies the failed fan number(s).						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔	✔	✔	✔	✔	✔	

Event Code: 306							
Message:	A cooling fan propeller in Fan2 FRU type has failed.						
Severity:	Major.						
Explanation:	The first of two fan propellers is no longer operational. The remainder of the fan propellers in the FAN2 FRU are operational. If present the LED on the associated fan module is turned off. The event only applies to Fuji32 switches which has a mix of Fan and Fan2 devices. It is not an indication of the state of the FAN single blade FRUs.						
Action:	Replace the FAN2 FRU immediately.						
Event Data:	**Byte 0** = Failed fan blade number.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Event Code: 307							
Message:	A cooling fan propeller in Fan2 FRU type has failed.						
Severity:	Major.						
Explanation:	The second of two fan propellers is no longer operational. Both propellers have failed or the FRU has been removed. The LED on the associated fan module is turned off. The event only applies to Fuji32 switches, which has a mix of Fan and Fan2 devices. It is not an indication of the state of the FAN single blade FRUs.						
Action:	Replace the FAN2 FRU immediately.						
Event Data:	Byte 0 = Failed fan blade number						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Event code: 310							
Message:	Cooling fan propeller recovered.						
Severity:	Informational.						
Explanation:	One cooling fan recovered or the associated power supply was replaced.						
Action:	No action required.						
Event data:	The first byte of event data (byte **0**) specifies the recovered fan number.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Event code: 311	
Message:	Cooling fan propeller recovered.
Severity:	Informational.

Explanation:	Two cooling fans recovered or the associated power supply was replaced.						
Action:	No action required.						
Event data:	The first byte of event data (byte **0**) specifies the recovered fan number(s).						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Event code: 312							
Message:	Cooling fan propeller recovered.						
Severity:	Informational.						
Explanation:	Three cooling fans recovered or the associated power supply was replaced.						
Action:	No action required.						
Event data:	The first byte of event data (byte **0**) specifies the recovered fan number(s).						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Event code: 313	
Message:	Cooling fan propeller recovered.
Severity:	Informational.
Explanation:	Four cooling fans recovered or both power supplies were replaced.
Action:	No action required.
Event data:	The first byte of event data (byte **0**) specifies the recovered fan number(s).

Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Event code: 314							
Message:	Cooling fan propeller recovered.						
Severity:	Informational.						
Explanation:	Five cooling fans recovered or both power supplies were replaced.						
Action:	No action required.						
Event data:	The first byte of event data (byte **0**) specifies the recovered fan number(s).						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Event code: 315							
Message:	Cooling fan propeller recovered.						
Severity:	Informational.						
Explanation:	Six cooling fans recovered or both power supplies were replaced.						
Action:	No action required.						
Event data:	The first byte of event data (byte **0**) specifies the recovered fan number(s).						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Event Code: 316							
Message:	A cooling fan propeller in FAN2 FRU has recovered.						
Severity:	Informational.						
Explanation:	A fan propeller started spinning. It either spontaneously recovered or its FRU was replaced. One propeller in FAN2 FRU is now operational.						
Action:	No action required.						
Event Data:	**Byte 0** = Recovered fan blade number.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✔		✔				

Event Code: 317							
Message:	A cooling fan propeller in FAN2 FRU has recovered.						
Severity:	Informational.						
Explanation:	A fan propeller started spinning. It either spontaneously recovered or its FRU was replaced. Two propellers in FAN2 FRU are now operational.						
Action:	No action required.						
Event Data:	**Byte 0** = Recovered fan blade number.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✔		✔				

Event code: 370	
Message:	Cooling fan status polling temporarily disabled.
Severity:	Minor.

Explanation:	The failed or recovered status values for one or more cooling fans are exceeding a determined threshold. This indicates a possible fan failure. Fan status polling is enabled hourly or following an IML or reset.						
Action:	No immediate action required. Monitor cooling fan operation or additional event codes indicating a fan failure.						
Event data:	No supplementary data included.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔	✔	✔	✔	✔		

CTP card events (400 through 499)

Event code: 400							
Message:	Power-up diagnostics failure.						
Severity:	Major.						
Explanation:	Power-on self tests (POSTs) detected a failed CRU as indicated by the event data.						
Action:	If a CTP card failure is indicated, replace the switch. If a fan or power supply failure is indicated, contact IBM to replace the power supply. Perform a data collection and return the CD and faulty FRU to support personnel.						
Event data:	Byte **0** = CRU code as follows: **02** = CTP card, **05** = cooling fan, **06** = power supply assembly. Byte **1** = CRU slot number.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔	✔	✔	✔	✔	✔	

Event code: 410							
Message:	Switch reset.						
Severity:	Informational.						
Explanation:	The switch reset due to system power-up, IML, or manual reset. A software reset can occur automatically after a firmware fault (event code **411**), or be user-initiated. Event data indicates the type of reset.						
Action:	No action required.						
Event data:	Byte **0** = reset type as follows: **00** = power-on, **02** = IML, **04** = reset.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Event code: 411							
Message:	Firmware fault.						
Severity:	Major.						
Explanation:	Switch firmware encountered an unexpected condition and dumped operating state information to FLASH memory for retrieval and analysis. The dump file automatically transfers to the management server, where it is stored for retrieval through a data collection. The switch performs a software reset, during which all attached Fibre Channel devices are momentarily disrupted, log out, and log back in.						
Action:	Perform a data collection and return the CD to support personnel.						
Event data:	Bytes **0** - **3** = fault identifier, least significant byte first.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔	✔	✔	✔	✔	✔	

Event code: 421							
Message:	Firmware download complete.						
Severity:	Informational.						
Explanation:	A new firmware version was downloaded from the management server or EFCM Basic interface. Event data contains the ASCII firmware version in hexadecimal format **xx.yy.zz.bbbb**.						
Action:	No action required.						
Event data:	Bytes **0** and **1** = release level (**xx**). Byte **2** = always a period. Bytes **3** and **4** = maintenance level (**yy**). Byte **5** = always a period. Bytes **6** and **7** = interim release level (**zz**). Byte **8** = always a space. Bytes **9** - **12** = build ID (**bbbb**).						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Event code: 423							
Message:	CTP firmware download initiated.						
Severity:	Informational.						
Explanation:	The management server or EFCM Basic Edition interface initiated download of a new firmware version.						
Action:	No action required.						
Event data:	No supplementary data included.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Event Code: 430	
Message:	Excessive Ethernet transmit errors.
Severity:	Informational.
Explanation:	Transmit error counters for the active CTP card Ethernet adapter (sum of all counters) exceeded a threshold. This does not indicate a CTP card failure; it indicates a problem with the Ethernet cable, hub, or device on the same Ethernet segment. Event data counters are represented in hexadecimal format with the least significant byte first.
Action:	Verify the Ethernet cable, hub, and other devices are properly connected and operational.
Event Data:	Bytes **0** - **3** = sum of all transmit errors (total_xmit_error). Bytes **4** - **7** = frame count where Ethernet adapter does not detect carrier sense at preamble end (loss_of_CRSs_cnt). Bytes **8** - **11** = frame count where Ethernet adapter does not detect a collision within 64 bit times at transmission end (SQE_error_cnt). Bytes **12** - **15** = frame count where Ethernet adapter detects a collision more than 512 bit times after first preamble bit (out_of_window_cnt). Frame not transmitted. Bytes **16** - **19** = frame count where transmission is more than 26 ms (jabber_cnt). Frame not transmitted. Bytes **20** - **23** = frame count where Ethernet adapter encounters 16 collisions while attempting to transmit a frame (16coll_cnt). Frame not transmitted.

Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✔		✔				

Event Code: 431	
Message:	Excessive Ethernet receive errors.
Severity:	Informational.
Explanation:	Receive error counters for the active CTP card Ethernet adapter (sum of all counters) exceeded a threshold. This does not indicate a CTP card failure; it indicates a problem with the Ethernet cable, hub, or device on the same Ethernet segment. Event data counters are represented in hexadecimal format with the least significant byte first.
Action:	Verify the Ethernet cable, hub, and other devices are properly connected and operational.
Event Data:	Bytes **0** - **3** = sum of all receive errors (total_recv_error). Bytes **4** - **7** = frame count where received frame had from 1 to 7 bits after last received full byte (dribble_bits_cnt). CRC error counter updated but frame not processed. Bytes **8** - **11** = frame count where received frame had bad CRC (CRC_error_cnt). Frame not processed. Bytes **12** - **15** = frame count received with less than 64 bytes (runt_cnt). Broadcast frames count but do not contribute to threshold. Frame not processed. Bytes **16** - **19** = frame count received with more than 1518 bytes (extra_data_cnt). Broadcast frames count but do not contribute to threshold. Frame not processed.

Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✔		✔				

Event Code: 432	
Message:	Ethernet adapter reset.
Severity:	Minor.
Explanation:	The active CTP card Ethernet adapter was reset in response to an internally detected error. A card failure is not indicated. The director-to-management server connection terminates, but automatically recovers after the reset.
Action:	Perform the data collection procedure and return the CD to support personnel.

Event Data:	Bytes **0** - **3** = reason for adapter reset, least significant byte first (reset_error_type) **1** = completion notification for timed-out frame transmission.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✔		✔				

Event code: 433							
Message:	Nonrecoverable Ethernet fault.						
Severity:	Major.						
Explanation:	A non-recoverable Ethernet interface failure was detected and the LAN connection to the management server or Internet was terminated. No failure information or event codes are reported outside the switch. Although Fibre Channel port functionality is not affected, the switch cannot be monitored or configured.						
Action:	Replace the switch.						
Event data:	Byte **0** = LAN error type as follows: **01** = hard failure, **04** = registered fault. Byte **1** = LAN error subtype (internally defined). Byte **2** = LAN fault identifier (internally defined).						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔	✔				✔	

Event code: 440	
Message:	Embedded port hardware failed.
Severity:	Major.
Explanation:	The embedded port hardware detected a fatal error.
Action:	Replace the switch.
Event data:	Byte **0** = CTP slot position (**00**). Byte **1** = engineering reason code Bytes **4** - **7** = elapsed millisecond tick count.

Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔	✔	✔	✔	✔	✔	

Event code: 442							
Message:	Embedded port anomaly detected.						
Severity:	Informational.						
Explanation:	The switch detected a deviation in the normal operating mode or status of the embedded port.						
Action:	No action required. An additional event code is generated if this incident exceeds an error threshold or results in a port failure.						
Event data:	Byte **0** = embedded port number. Byte **1** = anomaly reason code. Bytes **4** - **7** = elapsed millisecond tick count. Bytes **8** and **9** = HA error callout #1. Bytes **10** and **11** = HA error callout #2. Byte **12** = detecting port. Byte **13** = connected port. Bytes **16** and **17** = HA error callout #3. Bytes **18** and **19** = HA error callout #4.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Port events (500 through 599)

Event Code: 502							
Message:	Port module anomaly detected.						
Severity:	Informational.						
Explanation:	The CTP card detected a deviation in the normal operating mode or status of the indicated four-port UPM.						
Action:	No action required. An event code **504** is generated if the UPM fails.						
Event Data:	Byte **0** = UPM slot position. Byte **1** = engineering reason code. Bytes **4** - **7** = elapsed millisecond tick count. Bytes **8** and **9** = high-availability error callout #1. Bytes **10** and **11** = high-availability error callout #2. Byte **14** = participating SBAR. Bytes **16** and **17** = high-availability error callout #3. Bytes **18** and **19** = high-availability error callout #4.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✔		✔				

Event Code: 504	
Message:	Port module failure.
Severity:	Major.
Explanation:	The indicated UPM failed.
Action:	Replace the indicated UPM with a functional UPM of the same type. Perform the data collection procedure and return the CD and faulty card to support personnel.
Event Data:	Byte **0** = UPM slot position Byte **1** = engineering reason code. Bytes **4** - **7** = elapsed millisecond tick count. Bytes **8** - **11** = reason code specific data.

Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Event Code: 505							
Message:	Port module revision not supported.						
Severity:	Minor.						
Explanation:	The indicated UPM is not recognized and the four ports appear uninstalled to the director firmware.						
Action:	Ensure the director model supports the operating firmware version. If the firmware version is supported, replace the UPM with a functional card. Perform the data collection procedure and return the CD and faulty card to support personnel.						
Event Data:	Byte **0** = UPM slot position). Bytes **4** - **7** = elapsed millisecond tick count. Bytes **8** and **9** = detected module identifier.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✔		✔				

Event code: 506	
Message:	Fibre Channel port failure.
Severity:	Major.
Explanation:	A Fibre channel port failed. The amber LED corresponding to the port illuminates to indicate the failure. Ports with LEDs extinguished remain operational.
Action:	Perform a a data collection and return the CD to support personnel. Perform a switch reset. If the problem persists, replace the switch.

Event data:	Byte **0** = port number. Byte **1** = engineering reason code. Bytes **4** - **7** = elapsed millisecond tick count. Bytes **8** - **11** = reason code specific. Byte **16** = connector type.				Bytes **17** and **18** = transmitter technology. Byte **19** = distance capability. Byte **20** = supported transmission media. Byte **21** and **22** = speed capability.		
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔	✔	✔	✔	✔	✔	

Event code: 507							
Message:	Loopback diagnostics port failure.						
Severity:	Informational.						
Explanation:	A loopback diagnostic test detected a Fibre Channel port failure.						
Action:	No action required. An event code **506** is generated if this diagnostic failure results in a hard port failure.						
Event data:	Byte **0** = port number. Byte **1** = engineering reason code. Bytes **4** - **7** = elapsed millisecond tick count.				Bytes **8** - **11** = reason code specific. Byte **12** = test type.		
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Event code: 508	
Message:	Fibre Channel port anomaly detected.
Severity:	Informational.
Explanation:	The switch detected a deviation in the normal operating mode or status of the indicated Fibre Channel port.
Action:	No action required. An event code **506** is generated if this anomaly results in a hard port failure.

Event data:	Byte **0** = port number. Byte **1** = anomaly reason code. Bytes **4** - **7** = elapsed millisecond tick count. Bytes **8** and **9** = HA error callout #1. Bytes **10** and **11** = HA error callout #2.			Byte **12** = detecting port. Byte **13** = connected port. Bytes **16** and **17** = HA error callout #3. Bytes **18** and **19** = HA error callout #4.			
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Event code: 510							
Message:	Optical transceiver hot-insertion initiated.						
Severity:	Informational.						
Explanation:	Installation of an optical transceiver was initiated with the switch powered on and operational. The event indicates operational firmware detected the presence of the transceiver.						
Action:	No action required.						
Event data:	Byte **0** = port number. Byte **2** = optic type. Bytes **4** - **7** = elapsed millisecond tick count. Bytes **8** - **11** = optic serial number.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Event code: 512	
Message:	Optical transceiver nonfatal error.
Severity:	Minor.
Explanation:	Switch firmware detected an optical transceiver non-fatal error.
Action:	Replace the failed transceiver with a functional transceiver of the same type.

Event data:	Byte **0** = port number. Byte **1** = engineering reason code. Byte **2** = optic type. Bytes **4** - **7** = elapsed millisecond tick count. Bytes **8** - **11** = optic serial number.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Event code: 513							
Message:	Optical transceiver hot-removal completed.						
Severity:	Informational.						
Explanation:	An optical transceiver was removed while the switch was powered on and operational.						
Action:	No action required.						
Event data:	Byte **0** = port number. Byte **2** = optic type. Bytes **4** - **7** = elapsed millisecond tick count. Bytes **8** - **11** = optic serial number.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔		✔				

Event code: 514	
Message:	Optical transceiver failure.
Severity:	Major.
Explanation:	An optical transceiver failed. The amber LED corresponding to the port illuminates to indicate the failure. Ports with LEDs extinguished remain operational.
Action:	Replace the failed transceiver.

Event data:	Byte **0** = port number. Byte **1** = engineering reason code. Byte **2** = optic type. Bytes **4** - **7** = elapsed millisecond tick count. Bytes **8** - **11** = optic serial number.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔	✔	✔	✔	✔	✔	

Event code: 581							
Message:	Implicit incident.						
Severity:	Major.						
Explanation:	An attached server recognized a condition caused by an event that occurred at the server. The event caused an implicit Fibre Channel link incident.						
Action:	A link incident record (LIR) is generated and sent to the attached server using the reporting procedure defined in T11/99-017v0 (OSI). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. Go to *MAP 0000: Start MAP* to perform fault isolation. In addition, perform a data collection and return the CD to support personnel.						
Event data:	Refer to the T11/99-017v0 document for the specific link incident record format.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
							✔

Event code: 582	
Message:	Bit error threshold exceeded.
Severity:	Major.
Explanation:	An attached server determined the number of code violation errors recognized exceeded the bit error threshold.
Action:	A LIR is generated and sent to the attached server using the reporting procedure defined in T11/99-017v0 (OSI). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. Go to *MAP 0000: Start MAP* to perform fault isolation. In addition, perform a data collection and return the CD to support personnel.

Event data:	Refer to the T11/99-017v0 document for the specific link incident record format.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
							✔

Event code: 583							
Message:	Loss of signal or loss of synchronization.						
Severity:	Major.						
Explanation:	An attached server recognized a loss-of-signal condition or a loss-of-synchronization condition that persisted for more than the specified receiver-transmitter timeout value (R_T_TOV).						
Action:	A LIR is generated and sent to the attached server using the reporting procedure defined in T11/99-017v0 (OSI). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. Go to *MAP 0000: Start MAP* to perform fault isolation. In addition, perform a data collection and return the CD to support personnel.						
Event data:	Refer to the T11/99-017v0 document for the specific link incident record format.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
							✔

Event code: 584							
Message:	Not operational primitive sequence received.						
Severity:	Major.						
Explanation:	An attached server received a not-operational primitive sequence (NOS).						
Action:	A LIR is generated and sent to the attached server using the reporting procedure defined in T11/99-017v0 (OSI). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. Go to *MAP 0000: Start MAP* to perform fault isolation. In addition, perform a data collection and return the CD to support personnel.						
Event data:	Refer to the T11/99-017v0 document for the specific link incident record format.						

Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
							✔

Event code: 585	
Message:	Primitive sequence timeout.
Severity:	Major.
Explanation:	An attached server recognized either a link reset (LR) protocol timeout or a timeout while waiting for the appropriate response (while in a NOS receive state and after NOS was not longer recognized).
Action:	A LIR is generated and sent to the attached server using the reporting procedure defined in T11/99-017v0 (OSI). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. Go to *MAP 0000: Start MAP* to perform fault isolation. In addition, perform a data collection and return the CD to support personnel.
Event data:	Refer to the T11/99-017v0 document for the specific link incident record format.

Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
							✔

Event code: 586	
Message:	Invalid primitive sequence received for current link state.
Severity:	Major.
Explanation:	An attached server recognized either a link reset (LR) or a link-reset response (LRR) sequence while in the wait-for-online sequence (OLS) state.
Action:	A LIR is generated and sent to the attached server using the reporting procedure defined in T11/99-017v0 (OSI). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. Go to *MAP 0000: Start MAP* to perform fault isolation. In addition, perform a data collection and return the CD to support personnel.
Event data:	Refer to the T11/99-017v0 document for the specific link incident record format.

Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
							✔

SBAR Events (600 through 699)

Event Code: 602							
Message:	SBAR anomaly detected.						
Severity:	Informational.						
Explanation:	Director operational firmware detected a deviation in the normal operating mode or operating status of the indicated SBAR.						
Action:	No action required. An event code **604** is generated if the SBAR fails.						
Event Data:	Byte **0** = SBAR slot position. Byte **1** = anomaly reason code. Bytes **4** - **7** = elapsed millisecond tick count. Bytes **8** and **9** = high-availability error callout #1. Bytes **10** and **11** = high-availability error callout #2.			Byte **12** = detecting port. Byte **13** = connected port. Byte **14** = participating SBAR. Bytes **16** and **17** = high-availability error callout #3. Bytes **18** and **19** = high-availability error callout #4.			
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✔		✔				

Event Code: 604	
Message:	SBAR failure.
Severity:	Major.
Explanation:	The indicated SBAR failed. If the active SBAR fails, the backup SBAR takes over operation. If the backup SBAR fails, the active SBAR is not impacted.
Action:	Replace the failed SBAR with a functional assembly. Perform the data collection procedure and return the CD and faulty assembly to support personnel.
Event Data:	Byte **0** = SBAR slot position. Byte **1** = engineering failure reason code. Bytes **4** - **7** = elapsed millisecond tick count. Bytes **8** - **11** = event code specific data.

Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Event Code: 605							
Message:	SBAR revision not supported.						
Severity:	Minor.						
Explanation:	The indicated SBAR is not recognized and appears uninstalled to the director firmware.						
Action:	Ensure the director model supports the operating firmware version. If the firmware version is supported, replace the SBAR with a functional assembly. Perform the data collection procedure and return the CD and faulty assembly to support personnel.						
Event Data:	Byte **0** = SBAR slot position. Bytes **4** - **7** = elapsed millisecond tick count. Bytes **8** and **9** = detected module identifier.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✔		✔				

Thermal sensor events (800 through 899)

Event Code: 800							
Message:	High temperature warning (port module thermal sensor).						
Severity:	Major.						
Explanation:	The thermal sensor associated with a UPM indicates the warm temperature threshold was reached or exceeded.						
Action:	Replace the indicated UPM with a functional UPM of the same type. Perform the data collection procedure and return the CD and faulty card to support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Event Code: 801							
Message:	Critically hot temperature warning (port module thermal sensor).						
Severity:	Major.						
Explanation:	The thermal sensor associated with a UPM indicates the hot temperature threshold was reached or exceeded.						
Action:	Replace the indicated UPM with a functional UPM of the same type. Perform the data collection procedure and return the CD and faulty card to support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Event Code: 802							
Message:	Port module shutdown due to thermal violation.						
Severity:	Major.						
Explanation:	A UPM failed and was powered off because of excessive heat. This event follows an indication that the hot temperature threshold was reached or exceeded (event code **801**).						
Action:	Replace the failed UPM with a functional UPM of the same type. Perform the data collection procedure and return the CD and faulty card to support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Event Code: 805							
Message:	High temperature warning (SBAR thermal sensor).						
Severity:	Major.						
Explanation:	The thermal sensor associated with an SBAR indicates the warm temperature threshold was reached or exceeded.						
Action:	Replace the indicated SBAR with a functional assembly. Perform the data collection procedure and return the CD and faulty assembly to support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Event Code: 806							
Message:	Critically hot temperature warning (SBAR thermal sensor).						
Severity:	Major.						
Explanation:	The thermal sensor associated with an SBAR indicates the hot temperature threshold was reached or exceeded.						
Action:	Replace the indicated SBAR with a functional assembly. Perform the data collection procedure and return the CD and faulty assembly to support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Event Code: 807							
Message:	SBAR shutdown due to thermal violation.						
Severity:	Major.						
Explanation:	An SBAR failed and was powered off because of excessive heat. This event follows an indication that the hot temperature threshold was reached or exceeded (event code **806**). If the active SBAR fails, the backup SBAR takes over operation. If the backup SBAR fails, the active SBAR is not impacted.						
Action:	Replace the failed SBAR with a functional assembly. Perform the data collection procedure and return the CD and faulty assembly to support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Director		Management Server			Host	
	Nonvolatile System Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Event code: 810							
Message:	High temperature warning (CTP card thermal sensor).						
Severity:	Major.						
Explanation:	The thermal sensor associated with the CTP card indicates the warm temperature threshold was reached or exceeded.						
Action:	Perform a data collection and return the CD to support personnel. Perform a switch reset. If the problem persists, replace the switch.						
Event data:	No supplementary data included.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔	✔	✔	✔	✔	✔	

Event code: 811							
Message:	Critically hot temperature warning (CTP card thermal sensor).						
Severity:	Major.						
Explanation:	The thermal sensor associated with the CTP card indicates the hot temperature threshold was reached or exceeded.						
Action:	Perform a data collection and return the CD to support personnel. Perform a switch reset. If the problem persists, replace the switch.						
Event data:	No supplementary data included.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔	✔	✔	✔	✔	✔	

Event code: 812							
Message:	CTP card shutdown due to thermal violations						
Severity:	Major.						
Explanation:	The CTP card failed due to excessive thermal violations. This event follows an event code **811**.						
Action:	Perform a data collection and return the CD to support personnel. Perform a switch reset. If the problem persists, replace the switch.						
Event data:	No supplementary data included.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔	✔	✔	✔	✔	✔	

Event code: 850							
Message:	Switch shutdown due to CTP thermal violations						
Severity:	Severe.						
Explanation:	The switch failed due to excessive CTP card thermal violations.						
Action:	Perform a data collection and return the CD to support personnel. Perform a switch reset. If the problem persists, replace the switch.						
Event data:	No supplementary data included.						
Distribution:	Product		Management Server			Host	
	EFCM Basic Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident Log
	✔	✔	✔	✔	✔	✔	

Notices

This information was developed for products and services offered in the U. S. A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe on any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, N.Y. 10504-1785
U.S.A.

For additional information, visit the web at:

http://www.ibm.com/ibm/licensing/contact/

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

© Copyright IBM Corp. 2006

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM web sites are provided for convenience only and do not in any manner serve as an endorsement of those web sites. The materials at those web sites are not part of the materials for this IBM product and use of those web sites is at your own risk.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements, or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

If you are viewing this information in softcopy, the photographs and color illustrations may not appear.

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both: IBM, ESCON, eServer, FICON.

McDATA, EFC Manager, EFCM, Eclipse, OPENready, SANpilot, EFCM Basic, SANvergence, SANtegrity, Enterprise Operating System, E/OS, E/OSi, and E/OSn are trademarks of McDATA Corporation and its subsidiaries in the United States, other countries, or both.

Intel, MMX, and Pentium are trademarks of Intel Corporation in the United States, other countries, or both.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Linux is a trademark of Linus Torvalds.

Microsoft, Windows, and Windows NT® are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, or service names may be trademarks or service marks of others.

Electronic emission notices

The following statements apply to this product. The statements for other products intended for use with this product will appear in their accompanying manuals.

Federal Communications Commission (FCC) Class A Statement

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in

a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense. IBM is not responsible for any radio or television interference caused by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment. This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Industry Canada Class A Emission Compliance Statement

This Class A digital apparatus complies with Canadian ICES-003.

Avis de conformité à la réglementation d'Industrie Canada

Cet appareil numérique de la classe A est conform à la norme NMB-003 du Canada.

European Union (EU) Electromagnetic Compatibility Directive

This product is in conformity with the protection requirements of EU Council Directive 89/336/EEC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the fitting of non-IBM option cards. This product has been tested and found to comply with the limits for Class A Information Technology Equipment according to European Standard EN 55022. The limits for Class A equipment were derived for commercial and industrial environments to provide reasonable protection against interference with licensed communication equipment.

Attention: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures. Properly shielded and grounded cables and connectors must be used in order to reduce the potential for causing interference to radio and TV communications and to other electrical or electronic equipment. Such cables and connectors are available from IBM authorized dealers. IBM cannot accept

responsibility for any interference caused by using other than recommended cables and connectors.

Germany Electromagnetic Compatibility Directive

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Vertraglichkeit von Geraten (EMVG) vom 18. September 1998 (bzw. der EMC EG Richtlinie 89/336).

Dieses Gerät ist berechtigt, in Ubereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Konformitätserklarung nach Paragraph 5 des EMVG ist die: IBM Deutschland Informationssysteme GmbH 70548 Stuttgart. Informationen in Hinsicht EMVG Paragraph 4 Abs.

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 Klasse A.

EN 55022 Klasse A Geräte müssen mit folgendem Warnhinweis versehen werden: “Warnung: dies ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funkstorungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Masnahmen durchzuführen und dafür aufzukommen.”

Anmerkung: Um die Einhaltung des EMVG sicherzustellen, sind die Geräte wie in den IBM Handbüchern angegeben zu installieren und zu betreiben.

People’s Republic of China Class A Electronic Emission Statement

中华人民共和国“A类”警告声明

声 明

此为A级产品，在生活环境中，该产品可能会造成无线电干扰。在这种情况下，可能需要用户对其干扰采取切实可行的措施。

Korean Class A Electronic Emission Statement

이기기는 업무용으로 전자파 적합등록을 받은 기기
이오니, 판매자 또는 사용자는 이점을 주의하시기
바라며, 만약 잘못 구입하셨을 때에는 구입한 곳에
서 비업무용으로 교환하시기 바랍니다.

Japan VCCI Class A ITE Electronic Emission Statement

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に
基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を
引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求
されることがあります。

vcci

Index

A

access control list
  configure
    Element Manager 90
  description 90
authentication
  access control list 90
  configure
    EFCM Basic 45
    Element Manager 89
    SAN management application 89
  RADIUS server support 90
  settings 90
authentication settings
  configure
    Element Manager 90
  description 90

B

back up
  SAN management application configuration data 91
  switch configuration file
    EFCM Basic Edition 178
    SAN management application 206
BB_Credit
  configure
    EFCM Basic 36
    Element Manager 81
  description 36, 81
binding
  fabric
    configure through EFCM Basic 46
    configure through SAN management application 90
    enable through EFCM Basic 46
    enable through SAN management application 90
    Enterprise Fabric Mode 46, 90
  port
    configure through EFCM Basic 46
    enable through EFCM Basic 46
  switch
    configure through EFCM Basic 46
    configure through Element Manager 90
    enable through EFCM Basic 46
    enable through Element Manager 90
block port
  EFCM Basic Edition 175
  SAN management application 202

C

call-home support
  configure at management server 61, 89
  enable at management server 89
chassis ground connector
  description 6
  location 3
clean fiber-optic components 157
clearances 7
command line interface
  disable 39
  enable 39
configuration file
  back up
    EFCM Basic Edition 178
    SAN management application 206
  restore
    EFCM Basic Edition 179
    SAN management application 207
configure
  access control list
    Element Manager 90
  authentication settings
    Element Manager 90
  basic port information
    EFCM Basic 35
    Element Manager 80
  call-home feature 61
  call-home support 89
  Element Manager application 74
  e-mail notification 87
  Enterprise Fabric Mode
    EFCM Basic 46
    SAN management application 90
  Ethernet events 88
  fabric binding
    EFCM Basic 46
    SAN management application 90
  fabric parameters
    EFCM Basic 32
    Element Manager 78

© Copyright IBM Corp. 2006

ISL performance features
EFCM Basic 46
Element Manager 91
SAN management application 91
management server
date and time 59
DNS domain name 53
IP address 50
name 53
password 50
subnet mask 50
OpenTrunking
EFCM Basic 46
Element Manager 91
OSMS
EFCM Basic 39
Element Manager 70
passwords 51, 62
PFE keys
EFCM Basic 42
Element Manager 68
port BB_Credit
EFCM Basic 36
Element Manager 81
port binding
EFCM Basic 46
port fencing
EFCM Basic 47
SAN management application 91
port NPIV
EFCM Basic 37
Element Manager 82
preferred path
EFCM Basic 46
Element Manager 91
RADIUS server
Element Manager 90
SANtegrity authentication
EFCM Basic 45
Element Manager 89
SANtegrity binding
EFCM Basic 45
Element Manager 89
SAN management application 89
security features
EFCM Basic 45
Element Manager 89
SAN management application 89
SNMP
EFCM Basic 37
Element Manager 82
SSL encryption
software 40
web 40
switch binding
EFCM Basic 46
Element Manager 90
switch date and time
EFCM Basic 30
Element Manager 72
switch identification
EFCM Basic 29
Element Manager 75
switch network information
EFCM Basic 34
maintenance port 47
switch operating parameters
EFCM Basic 31
Element Manager 76
switch to SAN management application 64
threshold alerts 84
user names 62
Windows users 56
zone sets 95
zones 95
cooling fan
description 4
events (300 - 399) 258
fault isolation 123
illustrated parts breakdown 227
CRU removal
power supply 220
SFP transceiver 216
tools required 216
CRU replacement
power supply 222
SFP transceiver 218
tools required 216
CRUs
description 2
illustrated parts breakdown 225
power supply 4
SFP transceiver 3
status LEDs 6

CTP card
events (400 - 499) 266
fault isolation 123
firmware versions 176, 203

D

data collection procedure
EFCM Basic Edition 172
SAN management application 200
date
set at management server 59
set switch date
EFCM Basic 30
Element Manager 72
default
DNS server IP address 65
EFCM Basic Edition
password 27
user name 27
maintenance port password 49, 121
management server
gateway address 65
IP address 65
LCD panel password 51
subnet mask 65
SAN management application
password 62, 94
user name 62, 94
SAN management application password 213
SAN management application user name 213
switch
gateway address 17, 99
IP address 17, 99
passwords 17, 99
subnet mask 17, 99
TightVNC password 53, 93, 212
Windows
password 54, 94
user name 54, 94
Windows password 213
Windows user name 213
dimensions 7
door key
description 13
illustration 14
download
firmware from filecenter 158
software from filecenter 158
download firmware
EFCM Basic Edition 176
SAN management application 205

E

E_Port
configure 35, 80
description 1
OpenTrunking 46, 91
performance features 46, 91
port fencing 47, 91
preferred path 46, 91
segmented 141
e_port segmentation
reasons for 194
EFCM Basic Edition
configure product 27
embedded port frame log 163
event log 161
fabric log 163
link incident log 161
open trunking re-route log 162
EFCM Basic edition
disable at management server 86
enable at management server 86
Element Manager application
configure 74
configure PFE key
EFCM Basic 42
Element Manager 68
embedded port log 188
event log 185
hardware log 186
link incident log 186
open trunking log 187
port threshold alert log 186
switch fabric log 189
e-mail support
configure at management server 87
enable at management server 87
embedded port frame log
EFCM Basic Edition 163
embedded port log 188

enable
call-home support 89
command line interface 39
EFCM Basic edition 86
e-mail notification 87
Enterprise Fabric Mode
EFCM Basic 46
SAN management application 90
Ethernet events 88
host control
EFCM Basic 39
Element Manager 70
port binding
EFCM Basic 46
SSL encryption
software 40
web 40
switch binding
EFCM Basic 46
Element Manager 90
Telnet access 86
Enterprise Fabric Mode
configure
EFCM Basic 46
SAN management application 90
description 46, 90
enable
EFCM Basic 46
SAN management application 90
environment
operating 8
shipping 7
storage 7
equipment cabinet
description 1
switch installation 25
ERR LED
description 6
location 3
error detection
description 12
event codes 100
error reporting
description 12
event codes 100
ESD
RRP precautions 215
Ethernet connector
description 5
location 3
Ethernet events
configure at management server 88
enable at management server 88
Ethernet hub
description 11
fault isolation 113
illustration 11
installation 20
event codes
cooling fan events (300 - 399) 258
CTP card events (400 - 499) 266
description 233
port events (500 - 599) 272
power supply events (200 - 299) 254
system events (000 - 199) 234
thermal sensor events (800 - 899) 283
event log
EFCM Basic Edition 161
Element Manager 185
SAN management 182
external loopback test
description 171, 197
EFCM Basic Edition 171
SAN management application 197

F

F_Port
configure 35, 80
description 1
fabric binding
configure
EFCM Basic 46
SAN management application 90
description 46, 90
enable
EFCM Basic 46
SAN management application 90
Enterprise Fabric Mode 46, 90
fabric log
EFCM Basic Edition 163
SAN management 182
fabric parameters
configure

EFCM Basic 32
Element Manager 78
Fabricenter equipment cabinet
Ethernet hub installation 22
fault isolation
MAP 0000 - Start MAP 104
MAP 0100 - Power distribution analysis 109
MAP 0200 - POST failure analysis 111
MAP 0300 - Loss of server communication 113
MAP 0400 - FRU failure analysis 123
MAP 0500 - Port failure or link incident analysis 126
MAP 0600 - Fabric or ISL problem analysis 138
summary 99
fenced E_Port
description 146
fault isolation 138
fiber-optic protective plug
description 14
illustration 14
FICON management server
configure PFE key
EFCM Basic 42
Element Manager 68
filecenter
download firmware 158
download software 158
firmware
add version to management server library 204
determine version
EFCM Basic Edition 176
SAN management application 203
download
EFCM Basic Edition 176
SAN management application 205
download version from filecenter 158
FL_Port
configure 35, 80
description 1
Flexport Technology
configure PFE key
EFCM Basic 68
description 68
FRU, *see*CRU
full-volatility
configure PFE key
EFCM Basic 42
Element Manager 68
full-volatility feature
description 172, 200

G

gateway address
change switch address 34, 47
management server default 65
switch default 17, 99

H

hardware log 186

I

identification
configure
EFCM Basic 29
Element Manager 75
illustrated parts breakdown
front-accessible CRUs 226
power cords 229
rear-accessible CRUs 227
IML switch 156
installation tasks
summary 17
Task 1 - Verify installation requirements 19
Task 10 - Set management server date and time 59
Task 11 - Configure the call-home feature (optional) 61
Task 12 - Assign user names and passwords 62
Task 13 - Configure the product to the management application 64
Task 14 - Record or verify server restore information 65
Task 15 - Verify product-to-server communication 66
Task 16 - Configure PFE key (optional) 68
Task 17 - Configure management server (optional) 70
Task 18 - Set product date and time 72

Task 19 - Configure the Element Manager application 74
Task 2 - Unpack, inspect, and install the Ethernet hub (optional) 20
Task 20 - Back up configuration data 91
Task 21 - Cable Fibre Channel ports 94
Task 22 - Configure zoning (optional) 95
Task 23 - Connect product to a fabric element (optional) 96
Task 3 - Unpack, inspect, and install the product 24
Task 4 - Configure product at the EFCM Basic Edition interface (optional) 27
Task 5 - Configure product network information (optional) 47
Task 7 - Configure server password and network addresses 50
Task 8 - Configure management server information 53
Task 9 - Configure Windows operating system users 56
internal loopback test
description 169, 196
EFCM Basic Edition 169
SAN management application 196
interop mode 33
interswitch link
configure performance features
EFCM Basic 46
Element Manager 91
SAN management application 91
description 1
fault isolation 138
OpenTrunking 46, 91
port fencing 47, 91
preferred path 46, 91
IP address
change switch address 34, 47
DNS server default 65
management server default 65
switch default 17, 99

L

laser transceiver
description 3
illustrated parts breakdown 226
removal 216
replacement 218
types available 3
LCD panel
configure private server network addresses 51
configure public server network addresses 52
default password for management server 51
LEDs
ERR 6
port status 6
power supply status 6
PWR 6
link incident log
EFCM Basic Edition 161
Element Manager 186
logs
embedded port 188
embedded port frame (EFCM Basic) 163
event (EFCM Basic) 161
event (Element Manager) 185
event (SAN management) 182
fabric (EFCM Basic) 163
fabric (SAN management) 182
hardware 186
link incident (EFCM Basic) 161
link incident (Element Manager) 186
open trunking 187
open trunking re-route (EFCM Basic) 162
port threshold alert 186
product status 183
switch fabric 189
loopback plug
description 14
illustration 14
loopback test
external
EFCM Basic Edition 171
SAN management application 197
internal
EFCM Basic Edition 169
SAN management application 196

M

MAC address, switch 47

maintenance analysis procedures
MAP 0000 - Start MAP 104
MAP 0100 - Power distribution analysis 109
MAP 0200 - POST failure analysis 111
MAP 0300 - Loss of server communication 113
MAP 0400 - FRU failure analysis 123
MAP 0500 - Port failure or link incident analysis 126
MAP 0600 - Fabric or ISL problem analysis 138
summary 99
maintenance approach 8
maintenance port
configure switch network addresses 48
default password 49, 121
description 6
location 3
manage configuration data
EFCM Basic Edition 178
SAN management application 206
management
management server 9
management server
access through TightVNC 53
description 9
event code tables 233
fault isolation 113
LCD panel password 51
minimum specifications 10
recommended specifications 10
specifications 10, 11
multiswitch fabric
e_port segmentation
reasons for 194

N

N_Port ID virtualization
configure PFE key
EFCM Basic 42
Element Manager 69
network information
configure management server 50
configure switch
EFCM Basic 34
maintenance port 47
NPIV
configure
EFCM Basic 37
Element Manager 82
description 37, 82
null modem cable
description 14
illustration 15

O

open trunking log 187
open trunking re-route log
EFCM Basic Edition 162
open-systems management server
configure
EFCM Basic 39
Element Manager 70
OpenTrunking
configure
EFCM Basic 46
Element Manager 91
configure PFE key
EFCM Basic 43
Element Manager 69
description 46, 91
operating environment 8
operating parameters
configure
EFCM Basic 31
Element Manager 76

P

password
configure at management server 62
customer-level switch 17, 99
default
management server LCD panel 51
default EFCM Basic Edition 27
default maintenance port 49, 121
default SAN management application 62, 94, 213
default TightVNC 53, 93, 212
default Windows 54, 94, 213
maintenance-level switch 17, 99
performance statistics
Class 2

EFCM Basic Edition 169
Class 3
EFCM Basic Edition 169
error
EFCM Basic Edition 169
open trunking 169
traffic
EFCM Basic Edition 169
PFE keys
configure
EFCM Basic 42
Element Manager 68
Element Manager application 42, 68
FICON management server 42, 68
Flexport Technology 68
full-volatility 42, 68
N_Port ID virtualization 42, 69
OpenTrunking 43, 69
port binding
configure
EFCM Basic 46
description 46
enable
EFCM Basic 46
port fencing
configure
EFCM Basic 47
SAN management application 91
description 47, 91
port threshold alert log 186
ports
cabling 94
configurable types 1
configure basic information
EFCM Basic 35
Element Manager 80
configure BB_Credit
EFCM Basic 36
Element Manager 81
configure NPIV
EFCM Basic 37
Element Manager 82
E_Port fencing 47, 91
events (500 - 599) 272
LED diagnostics 159
performance statistics
EFCM Basic Edition 169
Element Manager application 191
port properties 193
port technology 194
SFP transceivers 3
status LEDs 6
swap ports 198
power cords
illustrated parts breakdown 229
power requirements 7
power supply
description 4
events (200 - 299) 254
fault isolation 109
illustrated parts breakdown 227
location 3
removal 220
replacement 222
status LED 6
power-off procedure 155
power-on procedure 153
preferred domain ID 77
preferred path
configure
EFCM Basic 46
Element Manager 91
description 46, 91
procedural notes 153
procedures
EFCM Basic Edition
block or unblock port 175
data collection 172
manage configuration data 178
obtain log information 160
set online state 174
upgrade firmware 176
Element Manager application
perform port diagnostics 190
installation 17
power-off 155
power-on 153
repair 153
SAN management application
block or unblock port 202
data collection 200
manage configuration data 206
obtain fabric log information 181
obtain switch log information 184

set online state 201
upgrade firmware 203
product status log 183
publications, related xiii
PWR LED
description 6
location 3

R

rack-mount installation
Ethernet hub 22
switch 25
RADIUS server
configure
Element Manager 90
description 90
related publications xiii
remove and replace procedures
CRU list 216, 220
ESD precautions 215
procedural notes 215
repair procedures
clean fiber-optic components 157
EFCM Basic Edition
block or unblock port 175
collect maintenance data 172
manage configuration data 178
obtain log information 160
set online state 174
upgrade firmware 176
Element Manager application
perform port diagnostics 190
IML or reset switch 155
install or upgrade software 210
overview 153
port LED diagnostics 159
power-off procedure 155
power-on procedure 153
SAN management application
block or unblock port 202
collect maintenance data 200
manage configuration data 206
obtain fabric log information 181
obtain switch log information 184
set online state 201
upgrade firmware 203
swap ports 198
rerouting delay 78
reset
configuration data
EFCM Basic Edition 180
SAN management application 207
switch 156
RESET button
function 5
location 3
restore
switch configuration file
EFCM Basic Edition 179
SAN management application 207

S

safety
ESD precautions 215
SAN management application
default
password 62, 94
user name 62, 94
default password 213
default user name 213
event log 182
fabric log 182
product status log 183
SAN32M-2
CRU removal and replacement 215
CRUs 2
description 1
illustrated parts breakdown 225
installation 24
maintenance approach 8
management 9
repair procedures 153
specifications 7
SANtegrity authentication
access control list 90
configure
EFCM Basic 45
Element Manager 89
RADIUS server support 90
settings 90
SANtegrity binding
configure

EFCM Basic 45
Element Manager 89
SAN management application 89
Enterprise Fabric Mode
configure through EFCM basic 46
configure through SAN management application 90
fabric binding
configure through EFCM basic 46
configure through SAN management application 90
port binding
configure through EFCM basic 46
switch binding
configure through EFCM basic 46
configure through Element Manager 90
security features
configure
EFCM Basic 45
Element Manager 89
SAN management application 89
Enterprise Fabric Mode 45, 89
SANtegrity authentication 45, 89
SANtegrity binding 45, 89
segmented E_Port
description 141
fault isolation 138
serviceability features 12
set online state
EFCM Basic Edition 174
SAN management application 201
SFP transceiver
description 3
fault isolation 126
illustrated parts breakdown 226
removal 216
replacement 218
types available 3
shipping environment 7
SNMP
configure
EFCM Basic 37
Element Manager 82
description 37, 82
software
download version from filecenter 158
install 210
upgrade 210
specifications
management server 10, 11
switch clearances 7
switch dimensions 7
switch power requirements 7
SSL encryption
configure software encryption 40
configure web encryption 40
storage environment 7
subnet mask
change switch value 34, 47
management server default 65
switch default 17, 99
swap ports 198
switch binding
configure
EFCM Basic 46
Element Manager 90
description 46, 90
enable
EFCM Basic 46
Element Manager 90
switch fabric log 189
switch priority 33
system events (000 - 199) 234

T

Telnet access
disable at management server 86
enable at management server 86
test
call-home support 89
e-mail notification 87
thermal sensor events (800 - 899) 283
threshold alert
port properties dialog box 194
reasons for 194
threshold alerts
configure 84
description 84
types 85
TightVNC
access management server 53
default password 53, 93, 212
time

set at management server 59
set switch time
EFCM Basic 30
Element Manager 72
tools and test equipment
CRU removal and replacement 216
supplied by service personnel 15

U

unblock port
EFCM Basic Edition 175
SAN management application 202
user name
configure at management server 62
default EFCM Basic Edition 27
default SAN management application 62, 94, 213
default Windows 54, 94, 213

V

verify
management server restore information 65
power supply replacement 223
SFP transceiver replacement 219
switch-to-server communication 66

W

Windows
configure users 56
default
password 54, 94
user name 54, 94
default password 213
default user name 213
WWN
port properties dialog box 193

Z

zone sets
configure
EFCM Basic 95
Element Manager 95
description 95
naming conventions 95
zones
configure
EFCM Basic 95
Element Manager 95
description 95
naming conventions 95

Readers' Comments — We'd Like to Hear from You

IBM TotalStorage SAN32M-2
Installation and Service Manual
Service information: 2026 / 432, 32E

Publication No. GC26-7763-03

We appreciate your comments about this publication. Please comment on specific errors or omissions, accuracy, organization, subject matter, or completeness of this book. The comments you send should pertain to only the information in this manual or product and the way in which the information is presented.

For technical questions and information about products and prices, please contact your IBM branch office, your IBM business partner, or your authorized remarketer.

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you. IBM or any other organizations will only use the personal information that you supply to contact you about the issues that you state on this form.

Comments:

Thank you for your support.

Submit your comments using one of these channels:

- Send your comments to the address on the reverse side of this form.

If you would like a response from IBM, please fill in the following information:

Name	Address
Company or Organization	
Phone No.	E-mail address

Readers' Comments — We'd Like to Hear from You
GC26-7763-03

Cut or Fold
Along Line

Fold and Tape | **Please do not staple** | Fold and Tape

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

International Business Machines Corporation
Information Development
Department GZW
9000 South Rita Road
Tucson, Arizona U.S.A. 85744-0002

Fold and Tape | **Please do not staple** | Fold and Tape

Cut or Fold
Along Line

Printed in USA

GC26-7763-03